Governance Studies at BROOKINGS

June 2014

Databuse and a Trusteeship Model of Consumer Protection in the Big Data Era

Benjamin Wittes & Wells C. Bennett

INTRODUCTION

Benjamin Wittes is a senior fellow in Governance Studies at The Brookings Institution. He co-founded and is the editor-in-chief of the Lawfare blog, which is devoted to sober and serious discussion of "Hard National Security Choices," and is a member of the Hoover Institution's Task Force on National Security and Law.

Wells C. Bennett is a Fellow in National Security Law at the Brookings Institution and Managing Editor of Lawfare.

How much does the relationship between individuals and the companies in which they entrust their data depend on the concept of "privacy?" And how much does the idea of privacy really tell us about what the government does, or ought to do, in seeking to shield consumers from Big Data harms?

There is reason to ask. Privacy is undeniably a deep value in our liberal society. But one can acknowledge its significance and its durability while also acknowledging its malleability. For privacy is also something of an intellectual rabbit hole, a notion so contested and ill-defined that it often offers little guidance to policymakers concerning the uses of personal information they should encourage, discourage, or forbid. Debates over privacy often descend into an angels-on-the-head-of-a-pin discussion. Groups organize around privacy. Companies speak reverently of privacy and have elaborate policies to deliver it—or to justify their manipulations of consumer data as consistent with it. Government officials commit to protecting privacy, even in the course of conducting massive surveillance programs. And we have come to expect as much, given the disagreement in many quarters over what privacy means. The invocation of privacy mostly serves to shift discussion, from announcing a value to addressing what that value requires. Privacy can tell a government or company what to name a certain policy after. But it doesn't answer many questions about how data ought to be handled.

Moreover, in its broadest conception, privacy also has a way of overpromising—of creating consumer expectations on which our market and political system will not, in fact, deliver. The term covers such a huge range of ground that it can, at times, suggest protections in excess of what regulators are empowered to enforce by law,

what legislators are proposing, and what companies are willing to provide consistent with their business models.

In 2011, one of us suggested that "technology's advance and the proliferation of personal data in the hands of third parties has left us with a conceptually outmoded debate, whose reliance on the concept of privacy does not usefully guide the public policy questions we face." Instead, the paper proposed thinking about massive individual data held in the hands of third-party companies with reference to a concept it termed "databuse," which it defined as:

> the malicious, reckless, negligent, or unjustified handling, collection, or use of a person's data in a fashion adverse to that person's interests and in the absence of that person's knowing consent. Databuse can occur in corporate, government, or individual handling of data. Our expectations against it are an assertion of a negative right, not a positive one. It is in some respects closer to the non-self-incrimination value of the Fifth Amendment than to the privacy value of the Fourth Amendment. It asks not to be left alone, only that we not be forced to be the agents of our own injury when we entrust our data to others. We are asking not necessarily that our data remain private; we are asking, rather, that they not be used as a sword against us without good reason.[1]

In the pages that follow, we attempt to apply this idea to a broad public policy problem, one with which government, industry, consumers and the privacy advocacy world have long grappled: that of defining the data protection obligations of for-profit companies, with respect to the handling of individual data, when they receive that data in the course of providing services to consumers without financial charge. In other words, we attempt to sketch out the duties that businesses like Google and Facebook owe to their users—though without drawing on any broad-brush concepts of privacy. Rather, we attempt to identify, amid the enormous range of values and proposed protections that people often stuff into privacy's capacious shell, a core of user protections that actually represent something like a consensus.

This core interestingly lacks a name in the English language. But the values and duties that make it up describe a relationship best seen as a form of trusteeship. A user's entrusting his or her personal data to a company in exchange for a service, we shall argue, conveys certain obligations to the corporate custodians of that person's data: obligations to keep it secure, obligations to be candid and straightforward with users about how their data is being exploited, obligations not to materially misrepresent their uses of user data, and obligations not to use them in fashions injurious to or materially adverse to the users' interests without their explicit consent. These obligations show up in nearly all privacy codes, in patterns of government enforcement, and in the privacy policies of the largest internet companies. It is failures of this sort of data trusteeship that we define as databuse. And we argue that protection against

1 Benjamin Wittes, Databuse: Digital Privacy and the Mosaic at 17 (April 1, 2011).

databuse—and not broader protections of more expansive, aspirational visions of privacy—should lie at the core of the relationship between individuals and the companies to whom they give data in exchange for services.

The first-party, data-in-trade-for-services relationship is not the *only* one that matters in the Big Data world. We specifically here put aside the question of how to understand the obligations of so-called "data brokers"—companies having no direct relationship to the people whose data they collect and sell.[2] The many vexing policy questions that arise from data brokers are different in character from those implicating the first-party relationship, and we leave them for another day.

Our essay proceeds in several steps: It first summarizes reasons why, as a concept, privacy is too broad and amorphous to usefully guide the problem of data voluntarily given to third parties who provide us services. We then attempt to narrow it, by identifying the concept of databuse as that core of the privacy spectrum about which broad consensus favors legal protection, one most easily explained in terms of the trusteeship obligations that corporations assume when they acquire large quantities of data about their customers. A second section then describes what trusteeship ought to look like in a first-party, services-in-exchange-for-data setting. Here we envision three categories of corporate uses of consumer data—one in which the interests of the corporation and that of the consumer are congruent, one in which the corporation benefits but the consumer does not suffer, and one in which the corporation benefits at the expense of the consumer's interests—and argue that private and public sanctions are best reserved for the third category.

As we explain in the paper's third section, this approach promises a narrower conception of privacy—narrower, at any rate, than the one the Federal Trade Commission has sometimes used, and that European regulators have used frequently. However, it better explains much of the Commission's enforcement activities and the White House's legislative proposals than does the broader concept of privacy. There's a reason for this, we suspect, and it's not just that the relevant law does not countenance enforcement in situations in which—however anxious privacy advocates may be on their behalf—consumers face no tangible harm.[3] It's also that while a broad societal consensus exists about the need to safeguard consumers against deceptive corporate behavior and corporate behavior that causes consumer harm, no similar

2 *See generally* FTC Report, Data Brokers: A Call for Transparency and Accountability (2014).

3 *See* 15 U.S.C. § 45(a)(1) (declaring unlawful "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]"); see also *FTC Policy Statement on Unfairness*, Letter from Federal Trade Commission to Senators Wendell H. Ford and John C. Danforth (Dec. 17, 1980) at 3 ("Unfairness Policy Statement") (construing the "unfair" prong of § 45(a)(1), and requiring "substantial injury" as a precondition to a finding of "unfairness," while noting that "[e]motional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."); *FTC Policy Statement on Deception*, Letter from Federal Trade Commission to Congressman John D. Dingell (Oct. 14, 1983) at 2 ("Deception Policy Statement") (construing the "deceptive" prong of § 45(a)(1), and stating that the Federal Trade Commission "will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.")

consensus exists that consumers require protection from voluntary exchanges of personal data in return for services, services that trade privacy for other goods. Indeed, judging by consumer behavior, a consensus has all but developed in the opposite direction: that we routinely regard such trades as promising tangible benefits in exchange for reasonable and manageable risks in a data-dependent society. That view informs the paper's fourth and final section, in which we offer some general comments regarding future consumer protection law.

I. PRIVACY, TRUSTEESHIP, AND DATABUSE

Our premise is straightforward: "privacy," while a pervasive rhetoric in the area of data handling and management, is actually not a great vocabulary for discussing corporate responsibilities and consumer protection in this area. Specifically, the word promises a great deal more than policymakers are prepared to deliver, and in some ways, it also promises more than consumers actually want.

The concept certainly was not inevitable as the reference point for discussions of individual rights with respect to the handling of data. It developed (as one of us explained in the prior "databuse" paper[4]) over time, in response to the obsolescence of previous legal constructions designed to shield individuals from government and one another.

The Constitution, for example, made no mention of privacy. The Constitution did not have to, because in the founding era, it was exceedingly difficult to invade privacy interests without also trespassing against personal property or impinging upon an individual's freedom of conscience or right to keep mum—areas well covered already by the First, Third, Fourth, and Fifth Amendments. This arrangement did not stand up over time, however, given technological advances. Because of those, notions of privacy started to decouple from property and other rights, first in our minds and ultimately in our law. We created privacy because technology left previous doctrines unable to describe the intrusions on our seclusion that we were feeling.

Ironically, today it is privacy itself that no longer adequately describes the violations people experience with respect to large caches of personal data held by others—and it describes those violations less and less well as time goes on. Much of the material that makes up these datasets, after all, involves records of events that take place in public, not in private. Much of this data is sensitive only in aggregation; it is often trivial in and of itself—and we consequently think little of giving it, or the rights to use it, away. As a legal matter, this sort of data by its nature involves material we have disclosed to others in exchange for some benefit, and it thus generally lies outside of the protections of the Fourth Amendment[5]—which does not cover the actions of non-governmental parties. What's more, we often give this information away with the understanding, implicit or explicit, that it will be aggregated and mined for what it might

4 See generally Databuse at 4-11.

5 United States v. Miller, 425 U.S. 435, 442-43 (1976).

say about us. It takes a feat of intellectual jujitsu to construct a cognizable and actionable set of privacy interests out of the amalgamation of public activities in which one has engaged knowingly, and which involved trades with strangers in exchange for benefits. The term privacy has become something of a crutch, a description of many different values of quite-different weights that neither accurately nor usefully depicts the harms we fear.

That is why privacy does not exactly capture our expectations with respect to private handling of our data by the companies to which we fork it over—at least to the extent that our behaviors in the marketplace reflect our expectations. It is why we do not seem to operationalize an expectation of non-disclosure or confidentiality in our actions. When one stops and contemplates what genuinely upsets us in the marketplace, broad conceptions of privacy—conceptions based on secrecy or non-disclosure of one's data—do not express it well at all. It's not just that we happily trade confidentiality and anonymity for convenience. It's that we seem to have no trouble with disclosures and uses of our data when they take place for our benefit. Huge numbers of consumers happily let the contents of their emails guide the advertising they receive from their email providers. We react with equanimity when companies use our purchase data to recommend further purchases or when they amalgamate data from multiple sources to provide us with the services we want. We do not punish companies that aggressively use our data for purposes of their own, so long as those uses do not cause us adverse consequences.

Were we truly concerned with the idea that another person has knowledge of these transactions, we would react to these and many other routine online actions more hostilely. We would not knowingly allow merchants to track our purchases in exchange for a small discount. We would not move aggressively away from the anonymity of cash transactions. Yet we have no trouble with outside entities handling, managing, and even using our data—as long as we derive some benefit or, at least, incur no harm as a result. Rather, we positively expect uses of our data that will benefit or protect us; we tolerate uses of them so long as the consequences to us are benign; and we object viscerally only where the use of our data has some adverse consequence for us. We react positively or negatively to the collection, storage, and use of our data, in other words, not in proportion to whether that data is used in a fashion that protects our privacy in any sort of broad understanding of the term, but in proportion to whether it is used for our benefit or to our detriment and critically, how seriously to our detriment. This is not traditional privacy we are asking for. It is something different. That something is protection against what we call databuse.

Think of databuse as that core of the privacy spectrum that is most modest in nature. Databuse is different from broader visions of privacy in that it does not presume as a starting point the non-disclosure, non-use, even quarantining from human eyes of data we have

willingly transacted in exchange for services.[6] It does not pretend that the companies to which we entrust our data should take it from us with no ambitions to use it for their own gain—or that there is something disreputable or inappropriate about their doing so. It does not begin with the assumption that there is some platonic ideal of seclusion that a company is bound to honor on our behalf, even if we don't want it or even if we prefer to have our data used to market us products we might want to buy. It does not assume we feel violated by the knowledge that others may have of our lives—particularly if others are machines and using that information to provide us services and conveniences we happen to want. It does not assume we want our fitness monitors to shield the number of steps we take from our friends or from people we have never met; it instead treats the dissemination of such data—in whole or in part—as an option we might or might not want to choose.

Rather, databuse asks only for protection against unwarranted harms associated with entrusting our data to large entities in exchange for services from them. It asks that the costs of our engagement with these companies not be a total loss of control of the bits and pieces of transactional, communications, and locational data that make up the fabric of our day-to-day lives. It asks, in short, that the companies be reasonable and honest custodians—trustees—of the material we have put in their hands. It acknowledges that they will use it for their own purposes. It asks only that those purposes do not conflict with our own purposes or come at our expense.

The idea of trusteeship is central here, in that it helps guide both consumer expectations and corporate behavior. A trustee in the usual sense is supposed to be a good steward of property belonging to somebody else. That means an obligation, first and foremost, to administer the trust in the interest of the beneficiary, according to the trust instrument's terms.[7] A trustee is bound to act prudently, with reasonable care, skill and caution,[8] and to keep beneficiaries reasonably informed, both about the trust's formation and its subsequent activities—including any changes to the trust's operation.[9]

The analogy between trusts and data-driven companies is, of course, imprecise. Facebook—as custodian of your data—is not under any obligation to act in your financial interests or to take only actions with your best interests in mind. You do not expect that. You know—and if you

6 Some companies have sought to offer customers a freestanding ability to make money from corporate uses of personal data—for example, by "giv[ing] users a cut of ad revenue." David Zax, "Is Personal Data the New Currency?" *MIT Technology Review,* (Nov. 30, 2011) (describing the now-defunct "Chime.In," a social networking site that split advertising sales with its members); see also Joshua Brustein, "Start-Ups Seek to Help Users Put a Price on Their Personal Data," The New York Times (Feb. 12, 2013) (describing early-stage efforts by companies to permit consumers to profit from data sales).

7 Restatement (Third) of Trusts § 78.

8 *Id.* § 77.

9 *Id.* § 82.

use Facebook, you probably do not mind—that Facebook is using your data, the many fields of information you have given about yourself, to route advertising to you and to sell access to you to advertisers. You probably *do* expect, however, that the custodians of your data will not take steps that are actively prejudicial to your security, at odds with the commitments they made to you in inducing the use of their services, or that they would deprive you of rudimentary control over the manner in which your data gets used. You probably do expect that if Google tells you it won't do X, that means that it won't do X. And you build a certain set of behaviors and risk planning—mostly subconsciously—around the confidence you develop in the security and honesty of the companies that hold your stuff.

The essence of *this* sort of trusteeship, in other words, is an obligation on the part of companies to handle data in an honest, secure, and straightforward fashion, one that does not injure consumers and that gives them reasonable information about and control over what is and is not being done with the data they provide. This can be teased out into distinct components.

There is nothing new about these components. They are familiar enough, given the policy world's long-running effort to convert vague privacy ideas into workable codes of behavior. That project can be traced back at least to the Fair Information Practice Principles ("FIPPs"), which were themselves largely derived from a 1973 report by the Department of Health, Education and Welfare on "Records, Computers, and the Rights of Citizens."[10] In the years since, scores of articles, privacy policies and government documents have drawn on the FIPPs.[11] Recently, the Obama administration has relied upon them in ticking off a checklist of do's and don'ts for companies holding significant volumes of consumer data.[12] Our own catalog of corporate responsibilities broadly overlaps with that of the Obama administration—and the government studies and reports and academic literature the administration has relied upon. As we shall show, they also reflect the set of expectations that, when companies fail to meet them, yield enforcement actions by the FTC. And they also reflect the commitments the major data-handling companies actually make to their users. In other words, the components of databuse are the parts of privacy about which we all basically agree.

---

10 *See* generally Department of Health, Education and Welfare Report, Records, Computers, and the Rights of Citizens at xx-xxi (1973) (advocating enactment of a five-part, federal "Code of Fair Information Practice").

11 Many of today's marquee privacy concepts—"privacy by design," for example—derive from Fair Information Practice Principles, build upon them, or are applied with reference to them. *See, e.g.,* Ann Cavoukian, Information & Privacy Commissioner, Ontario, Canada, *Privacy by Design: The 7 Foundational Principles* at 1, 4 (2009) (noting that "universal principles of the Fair Information Practices (FIPs) are affirmed by those of Privacy by Design, but go beyond them to seek the highest global standard possible," and that "visibility and transparency," a tenet of privacy by design, "tracks well to Fair Information Practices[.]"); *see also, e.g.*, FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 22 (2012) ("Final Report")(noting "broad support" for privacy by design concepts, and calling for their implementation by private companies).

12 *See generally* White House Report, Consumer Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012).

To name but a few of the consensus-backed principles: first, companies must take responsibility for the *secure storage, custody, and handling* of personal data so that the consumer is, in fact, giving his or her data only to those entities to which he or she actually agrees to give them.[13] Data breaches are a major source of risk for consumers, the cause of identity thefts, fraud, and all kinds of scams. Protecting data is no less an obligation for a company that asks individuals to entrust it with data than it is for a bank that asks for trust in storing private money. Many of the Federal Trade Commission's enforcement actions have involved allegations of negligent handling of data in a fashion that produces consumer harms—including, as the Commission has argued in a closely watched suit against Wyndham Hotels, harms caused when a company persistently fails to remedy known and systemic security risks.[14]

Second, companies must *never use consumer data in a fashion prejudicial to the interests of consumers*. Consumers are far more savvy than some privacy advocates imagine them to be, and we believe individuals are generally capable of making reasonable risk management choices about when to trade personal data—and subject themselves to targeted advertising—in exchange for services of value. These risk-management decisions, however, require a certain faith that businesses in question—while pursuing interests of their own—are not actively subverting the consumers' interests.

This point is complicated, because not everyone agrees about what it means to act in a fashion prejudicial to someone's interests. The particularly shy or reclusive person, after all, may regard the entire data-sharing culture as deeply offensive to her interests, whereas the person who regards herself as having no secrets and nothing to hide may well regard a wide range of data uses as perfectly fine. That said, there are some behaviors that clearly cross the line, wherever one reasonably draws it. An outright lie that induces someone to give over her personal identifying information is never acceptable, regardless of that person's feelings one

13 *See, e.g.*, Consumer Privacy in a Networked World at 19 (recommending consumer "right to secure and responsible handling of personal data."); Final Report at 24-26, 24 (recommending that companies "provide reasonable security for consumer data[,]"; noting recognition that the data security requirement is "well-settled."); Department of Commerce Report, Commercial Data Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework at 57 (2010) (advocating for "comprehensive commercial data security breach framework").

14 *See, e.g.,* First Amended Complaint for Injunctive and Other Relief, *Federal Trade Commission v. Wyndham Worldwide Corp. et al.,* No. CV 12-1365-PHX-PGR ¶ 40 (D. Ariz., Aug. 9, 2012) (alleging that unreasonable security practices lead to three data breaches, which in turn lead to the compromise of more than 619,000 consumer payment card account numbers, the export of some such numbers to a domain registered in Russia, fraudulent charges on consumer accounts, more than $10.6 million in fraud loss, and consumers' financial injury—including unreimbursed fraud charges and the loss of access to finances and credit); Memorandum Opinion, *Federal Trade Commission v. Wyndham Worldwide Corp. et al*., No. CV-1887-ES-JAD (D.N.J., April 7, 2014) (denying motion to dismiss); *see also, e.g.,* Complaint, *In the Matter of The TJX Companies, Inc.,* No. C-4227 ¶¶ 8-11 (July 29, 2008) (alleging that, because of shoddy security practices and repeated security breaches, banks claimed tens of millions in fraudulent charges, that payment and credit cards were cancelled, that consumers could not access credit or bank accounts until bank issued replacement cards, and that 455,000 consumers' personal identifying information was compromised).

way or the other.[15] Nobody would bless the out-and-out harvesting of data regarding minors absent parental consent either.[16] These are easy cases. In the less clear-cut ones, people will not agree in absolute terms about how to define prejudice to consumer interests. For that reason, it is critical to let individuals make their own choices both about whether to do business with a given company and, to the maximum extent possible, about what they do and do not permit that company to do with their data.

That means, third, requiring *honest and straightforward accounts by companies of how they use consumer data:*[17] what they do with it, how they monetize it, what they do not do with it. This does not mean an endless, legalistic "Terms of Service" document that nobody reads but simply clicks through. Such documents may be important from the standpoint of technical compliance with the law. But they do not reasonably inform the average consumer about what he can or cannot expect. It means, rather, simple, straightforward accounts of what use the company makes of consumer data. It also means not retroactively changing those rules and giving consumers reasonable notice when rules and defaults are going to change prospectively. Companies differ quite a bit in the degree of useful disclosure they give their users—and in the simplicity of those disclosures. Google and Facebook have both become rather fulsome, creating useful and simple disclosure pages. Other companies provide less information or obscure it more.

Fourth, it also means—to the maximum extent possible—*giving consumers control over those decisions as applied to them*.[18] This is not a binary rule, consumer control not being an on-off switch. It is a spectrum, and again, companies differ in the degree to which they give consumers control over the manner in which they use those consumers' data. Facebook now gives users fairly specific control over whom they want to share materials with.[19] Google offers users remarkably granular control over what sort of advertising they do and don't want

15 *See generally* 15 U.S.C. § 45(a)(1) and Deception Policy Statement (proscribing, among other things, material misrepresentations by companies to consumers).

16 *See generally* 15 U.S.C. §§ 6501-6506 and 16 C.F.R. Part 312 (prohibiting, among other things, knowing online collection of personal information from children aged thirteen and under).

17 *See* Consumer Privacy in a Networked World at 14 (recommending consumer "right to easily understandable and accessible information about privacy and security practices"); Final Report at viii (recommending, among other things, that companies "increase the transparency of their data practices," and that "privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."); Commercial Data Privacy and Innovation in the Internet Economy at 30 (arguing that information disclosed to consumers regarding companies' data practices should be "accessible, clear, meaningful, salient and comprehensible to its intended audience.")

18 *See* Consumer Privacy in a Networked World at 11 (recommending consumer "right to exercise control over what personal data companies collect from them and how they use it."); Final Report at i (observing that recommendations of simplified choice and enhanced transparency would "giv[e] consumers greater control over the collection and use of their personal data); Commercial Data Privacy and Innovation in the Internet Economy at 69 ("A key goal is to protect informed choice and to safeguard the ability of consumers to control access to personal information.").

19 *See, e.g.,* "Basic Privacy Settings & Tools," https://www.facebook.com/help/325807937506242/, "Advertising on Facebook," https://www.facebook.com/about/ads/#impact.

to see and to what extent they want advertising based on their recorded interests.[20] Apple, by contrast, offers only a crude ability to limit interest-based advertising.[21] The more control consumers have over who has access to their data and what the trustee company can do it with, the less capacity for databuse the relationship with that company has.

Finally, fifth, companies have an obligation to *honor the commitments they make to consumers regarding the handling of their data*.[22] Promising a whole lot of user control is worthless if the promises are not honored. And a great many of the Federal Trade Commission's enforcement actions naturally involve allegations of companies committing themselves to a set of practices and then failing to live up to them.[23]

Notice how much of conventional privacy this conception of the relationship leaves out. For starters, it leaves out nearly all of what one of us has termed "privacy as sentiment," that is, the way we feel when information about us is available to strangers and the sense that, quite apart from any tangible damage a disclosure might do us, our data is nobody else's business. Privacy as sentiment is central to much of the privacy literature today and has often played a role in the way the Commission talks about the subject, particularly with respect to its authority to urge best practices. It plays a huge role in European attitudes towards privacy. A related conception of privacy sees in it some kind of right against targeted advertising and behavioral profiling—at least in its more aggressive forms. And many commentators see in privacy as well some right to control our reputations.

At least as to companies with which the user has a direct relationship, the databuse conception largely throws all of this to the wolves. It requires honest, straightforward dealings by companies. It requires that the user have fair and reasonable opportunity to assess the impact on values and interests she might care about—privacy among them—of giving over her data to the company. But it ultimately acknowledges that targeted advertising is something she might want, or something she might not mind, and it considers her reputation ultimately her own responsibility to protect.

II. INTERESTS CONGRUENT AND CONFLICTING

Another somewhat simpler way to think about the spectrum between good trusteeship and databuse—simpler, at any rate, than checking a company's actions against a list of information

20 *See, e.g.*, "Ads Settings," https://www.google.com/settings/u/0/ads?hl=en&sig=ACi0TChbOZFvCL369bCG6d5hJYPJEECyqB9_hNgRM53YiNzLXgXTVZx8waORNIfvug0zVcZCZwivkcF1OI4tEh3eq5BIVCXunEchKZGC01vyOvYAhYtGPy-9EUx3hO2dHJ-xa_5Md_FGpaOzR7XvUCK360TtIF-duy-pkEYp3RUzQ6798J0LLrKM

21 *See, e.g.*, "How to opt out of interest-based ads from Iad," http://support.apple.com/kb/HT4228

22 *See* Footnote 14.

23 *See, e.g.*, Complaint, *In the Matter of Facebook, Inc.*, No. C-4365 ¶¶ 17-18 (July 27, 2012); Complaint, *In the Matter of Myspace LLC*, No. C-4369 ¶¶ 14-16, 21-28 (Aug. 30, 2012).

practice norms—is to examine the congruence or conflict between a consumer's interests and the company's interests in the handling of that consumer's data. Not all such uses are objectionable, after all. Many are beneficial to the consumer, the very essence of the service the company provides. We do business with Facebook and Twitter, after all, *so they can share our data* with our friends and people who are interested in what we have to say. Google Maps can tell you what roads are congested *because lots of phones are sending it geolocation data*—phones that may well include yours. Some uses of our data, in other words, actively serve or support our interests. By contrast, a company that collects consumer data in the course of providing a service and then monetizes that data in a fashion that exposes consumers to risks they didn't reasonably bargain for is a wholly different animal.

So let's consider three different general categories of data use by companies with direct relationships with their customers.

Category I involves situations in which the consumer's interests and the company's interests align. A company wants to use the data for a particular purpose, and a consumer either actively wants the company to use the data for that purpose or actively wants services that depend pervasively on those uses of data.

This first grouping derives in part from consumers' motivations for offering up their data in the first place. People sign up for Google applications, for example, for many different reasons. But certainly among them are obtaining a convenient mechanism for sending and receiving electronic mail through the cloud; searching the web; and figuring out, in real time, the most expeditious travel routes from one place to another, while circumventing accidents or high-traffic areas. All of these services necessarily entail a certain measure of data usage and processing by the company to which the data is given: a message's metadata must be exploited, and its contents electronically repackaged to facilitate the message's transmission from sender to intended recipient. And, in order to carry out its mission of directing you from one place to another, Google Maps likewise must obtain and compare your location to the underlying map and to data identifying bottlenecks, roadblocks, or other trip-relevant events—data it is often getting by providing similar services to other users. Examination of search data enables Google to suggest search terms once you start typing and to correct the spelling of search terms when you mistype. Another everyday example, this one involving a common commercial exchange: most people use credit cards, either for the convenience or to borrow money from the issuing banks—or both. The bank, in turn, periodically scans customer accounts—peeking at the patterns of transactions—for activity indicative of possible theft or fraud. Most consumers actively want these services.

The foregoing class of data handling manages simultaneously to advance both parties' interests, and in obvious ways. Because of Google's practices, the customer gets better

service from Google—or in some cases gets service at all. In critical respects, this is often not the use of data as a currency in exchange for the service. This is the use of data *in order to provide the service*. Similarly, in our banking hypothetical, snooping around for fraud and money-laundering reassures and protects the consumer, for so long as she has entrusted her hard-earned cash—and the data about her transactions—to Bank of America, for example. At the same time, ensuring its capacity to prevent financial nightmares helps to maintain or even bolster Bank of America's reputation—and thus, its market position relative to competitors—as well as to protect it against that portion of the fraud for which it may incur financial liability.

The paradigmatic Category I use thus results in an easily identifiable, win-win outcome for company and consumer alike. The tighter the link between a given use and the reason a user opts to fork over his data in the first place, the more likely that use is to fall within Category I. Category I activity generally does not raise the hackles of privacy advocates, and the pure Category I situation generally ought to draw the most minimal attention from policy-makers as well, and impose only the most minimal corporate duty to apprise the consumer of the details surrounding its activity. By way of illustration, UPS need not obtain permission before performing any electronic processes necessary to ensure a package's safe delivery; and PayPal likewise doesn't have to ask before it deploys its users' data in an exercise meant to beta test its latest security protocols.[24]

There are, of course, legitimate questions about the boundaries of Category I with respect to different companies. Some companies would argue that advertising activities should fall within Category I, as they are making money by matching consumers with goods and services they want to purchase. For some consumers, particularly with respect to companies whose products they particularly like, this may even be correct. Many people find Amazon's book recommendations, based on the customer's prior purchasing patterns, useful, after all. And a remarkable number of people click on Facebook that they "like" sponsored posts from advertisers. That said, we think as a general matter, advertising does not fit into Category I. Many people find it annoying, and most people—we suspect—regard it as a cost of doing business with companies, rather than an aim of the consumer in entering into the relationship. Most people don't buy magazines in order to read the ads, and they generally don't subscribe to Facebook to see the ads either.

24 This is but one application of the context principle, which the Obama administration has emphasized in its approach to consumer privacy. *See generally* Helen Nissenbaum, "Privacy as Contextual Integrity," 79 Wash. L. Rev. 1119 (2004); Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (2010); *see also* Consumer Privacy in a Networked World at 15-19 (advocating for consumers' right to expect that data collection and use will be handled in a manner consistent with the context in which consumers furnish their data); *see also* Final Report at 36 (stating that "[c]ompanies do not need to provide choice before collecting and using consumers' data for commonly accepted practices," including product fulfillment and fraud prevention.); Commercial Data Privacy and Innovation in the Internet Economy at 18 & n. 11 ("A wide variety of authorities recognize that information privacy depends on context and that expectations of privacy in the commercial context evolve.").

Rather, advertising is perhaps the prototypical example of **Category II**, which is composed of data uses that advance the company's interests, but that neither advance nor undercut the consumer's interests. This category scores a win for the business, but is value-neutral from the standpoint of the data's originator.

Along with advertising, a lot of the private sector's Big Data analytic work might come under Category II. Take an e-commerce site that scrutinizes a particular customer's historical purchasing habits, and draws inferences about her interests or needs so as to market particular products in the future to her or to others, to sensibly establish discount percentages, or to set inventory levels in a more economical way. Or consider a cloud-based e-mail system that examines, on an automated and anonymized basis, the text of users' sent and received messages in an effort to better populate the ad spaces that border the area where users draft and read their e-mails.

Neither the online shopper nor the e-mail account holder obviously benefits from the above scenarios. But there isn't any measurable injury to speak of, either. The consumer may like the ads, may find them annoying, or may look right through them and not care one way of the other. But in and of themselves, the ads neither advantage him nor do him harm. The end result is thus a wash for the consumer, and a win for the company.

Category II uses often bother some privacy activists—who have, for example, objected to Google's automatic scanning of message contents.[25] In our view, however, it is better understood as a perfectly reasonable data-in-exchange-for-service arrangement. This is particularly true when Category II uses follow reasonably from the context of a consumers' interaction with a company.[26] A hardware store need not provide notice, and obtain prior consent, before analyzing an individual's purchase history and, in light of it, offering him a discount on a particular power drill that his purchase history suggests he may want. The person expects that of a merchant with which she has an ongoing relationship. Similarly, people understand that targeted marketing is one of the reasons companies provide free services in exchange for consumer data, and they factor that reality into their decision to do business with those companies. As long as the companies are up front about what they are doing, this category of activity involves a set of judgments best regulated by consumer choice and preference.

25 Jon Healey, "Privacy Advocates Attack Gmail – Again – for Email Scanning," The Los Angeles Times (Aug. 15, 2013) (noting complaint by Consumer Watchdog, a consumer privacy organization, which challenged Google's scanning of messages sent to Google subscribers from non-Google subscribers); *see also* Order Granting In Part and Denying In Part Defendant's Motion to Dismiss, *In Re: Google Inc. Gmail Litigation*, No. 13-MD-02340-LHK (N.D. Cal., Sept. 26, 2013) (partially denying motion to dismiss where, among other things, plaintiffs alleged that Gmail's automated scanning protocols, as applied to inbound messages, had violated federal and state wiretapping laws).

26 *See* Footnote 24.

This area is a good example of the tendency of privacy rhetoric to overpromise with respect to the protections consumers really need—or want. Seen through the lens of broader visions of privacy, a lot of Category II activity may cause anxieties about having data "out there" and about Big Data companies knowing a lot about us and having the ability to profile us and create digital dossiers on us.[27] But seen through a more modest databuse lens, these are relationships into which a reasonable consumer might responsibly choose to enter into with reputable companies—indeed, they are choices that hundreds of millions of consumers *are* making every day worldwide. There is no particular reason to protect people preemptively from them.

Rather, databuse in our view can reasonably be defined as data uses in **Category III**, that is, those that run directly contrary to consumers' interests and either harm them discernibly, put them at serious and inherent risk of tangible harm, or run counter to past material representations made by the company to the consumer about things it would or would not do. One of us previously explained the right at the heart of databuse as a "right to not have your data rise up and attack you."[28] Category III includes data uses that advantage the corporate actor *at the expense of the interests of the consumer*. Category III activity should, in our view, provoke regulatory action and expose a company to injunction, civil penalty, or a money judgment—or even criminal prosecution, in the most egregious cases.

That makes Category III the most straightforward of our three-tiered scheme, and examples of it far easier to identify. A company can be justly tarred as a databuser and punished accordingly, when it violates the core promises of trusteeship that lie beneath the major policy statements that have increasingly undergirded this field for years now: when it breaks a material promise made to the people who gave the company its data—such as by using the data in a manner contradicted by a privacy policy or some other terms-establishing document; when the company stores its users' data in a less than reasonably safe way—such as by refusing to mitigate readily discoverable, significant cyber vulnerabilities, or by failing to enact industry-standard and business-appropriate security practices; or when the company deploys data in a fashion that otherwise threatens or causes tangible injury to its customers.

The critical question for a corporation of any real size providing free services to customers and exploiting their data is how to keep a healthy distance from Category III activities, while at the same time maximizing value. The answer has to do with the trusteeship obligations businesses incur when they strive to make profitable use of their customers' data. These often imply a greater threshold of care and protection than purely market-oriented principles do. The former is normative, in that it is designed to ensure a beneficiary's confidence and create

27 Preliminary FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: a Proposed Framework for Businesses and Policymakers at 20 (2012) ("Preliminary Report").

28 *Databuse* at 4.

conditions for the beneficiary's success. The latter is ambivalent, and thus suggests a just-do-the-least-required-to-further-one's-own-ends sort of regime. It would tolerate, for example, a minimally-adequate corporate policy about how data is collected, used, and disseminated, or permit that policy to be scattered about various pages of a website, nested in a Russian-doll-like array of click-through submenus or drowned in legalese or technical gobbledygook. The good data trustee is going to do something more fulsome than that. Companies engaged in good data trusteeship will provide prominent, readily-comprehensible explanations of their data practices, ones that fully equip the consumer to make informed choices about whether to do business or go elsewhere.[29]

The same idea holds true in other areas pertinent to the bilateral arrangement between the person contributing data and the company holding data. The market might require the company only to obtain a consumer's consent to its data practices once. A good data trustee is going to refresh that consent regularly by giving the user a lot of control for so long as the user's data resides with the company. Where the market might presume consent to most uses generally, a good data trustee will not, but will require additional consent for uses beyond those reasonably or necessarily following from the nature of the consumer's transaction with the company.[30]

It's easy to see what consumers get out of this vision, but what's in it for the companies? A lot. Trusteeship promises corporations the greatest possible measure of consumer confidence—and thus, a greater willingness to offer up more and more data for corporate use. As the Federal Trade Commission has reported, some of our economy's most data-deluged enterprises have found that the more choices they offer to their users in the first instance about whether to allow data exploitations, the more those users elect to remain "opted in" to features that use or disseminate data more broadly than the alternatives.[31] Getting people to give you large quantities of data requires, in the long run, their confidence. Good data trusteeship is critical to maintaining that confidence.

III. PRIVACY RHETORIC, DATABUSE ENFORCEMENT

Mario Cuomo once quipped that politicians "campaign in poetry" but "govern in prose."[32] There is a similar, if subtler disjuncture between the government's activities and some of its rhetoric, so far as concerns protecting consumers from Big Data harms. Policymakers often speak—and overpromise—in the broad language of privacy. But when the time comes to actually sue companies or to make actionable policy, they tend to take a narrower focus. They punish

29 *See* Footnote 17.

30 *See* Footnote 24.

31 Final Report at 9 & n. 40 (noting, among other things, comments from Google regarding its subscribers, who use Google's Ads Preference Manager and remain "opted in.").

32 Fred Barnes, "Meet Mario the Moderate," *The New Republic* at 18 (April 4, 1985).

behavior that looks a lot like databuse. In other words, there is a gap—sometimes modest, sometimes large—between the theoretical account in our politics of what we are protecting consumers from, and the sort of corporate behaviors that will actually trigger enforcement actions by regulators or senior-level calls for legislative reform. To put it simply, databuse better portrays what the government does, whatever it may say it wants to do, than do grander conceptions of privacy.

Consider the enforcement history of the Federal Trade Commission—the federal government's lead privacy agency. The FTC does not take action against companies whose practices merely impinge on user privacy in the broad sense in which some privacy advocates, and, indeed, the Commission itself, sometimes use the term. When companies have acted in a manner contrary to consumers' interests, however, the Commission has acted aggressively. Sometimes this has meant resorting to "sector-specific" laws, including those safeguarding data regarding creditworthiness, health, or finances; mostly, though, the Commission has brought suit under the Federal Trade Commission Act, arguing that companies have engaged in deceptive or unfair trade practices.

But the Commission typically limits enforcement to Category III scenarios. It holds off when corporate conduct fits best in Category I and, more interestingly, despite some stray rhetoric suggesting otherwise—which we note below—it also does not enforce against Category II behavior. Its enforcement division simply does not sue just because Big Data companies stir privacy fears. And it has yet to bring any action that does not allege, at a minimum, a material misrepresentation, data breach, or some other traditionally recognized form of consumer harm—but that instead seeks to remedy purely subjective injury or feeling. This should hardly come as a shock, given the Commission's longstanding position that deception or tangible harms are prerequisites for a viable lawsuit under its heartland consumer protection law. The Commission's practice, in other words, is to strike out not in defense of privacy in some broad sense, but instead against true failures of trusteeship in both the data-for-service and fee-for-service contexts.

To cite a few examples: In legal filings, the Commission repeatedly has alleged that various cloud outfits shirked the duty to tell consumers the truth, or at least not to mislead people who exchange their data for a good or service. It enforced against Facebook, for allegedly — telling members that, by opting for certain privacy settings, only "friends" could access the members' profile information, even though, according to the Commission, others indeed could access it.[33] It sued MySpace for allegedly telling its members that it would not share identifying information except as provided for in the company's privacy policy, and that the company complied with U.S.-E.U. safe harbor agreement, even though, according to the Commission, it had shared members' personal information more widely than represented and didn't at all

33 Complaint, *In the Matter of Facebook, Inc.,* No. C-4365 ¶¶ 17-18 (July 27, 2012).

comply with the international accord.[34] And it likewise sued Google, when the company had represented to Gmail users that their personal information would be used only in connection with the provision of web-based e-mail, even though, according to the Commission, Google had employed users' data in order to populate Google Buzz, a separate social networking tool—and thus permitted, in some cases, blocked individuals to "follow" users on Google Buzz.[35]

As discussed above, trustees also shoulder the responsibility of keeping their customers' data reasonably safe. And the Commission has enforced aggressively against companies that fail to do so. At the heart of the Commission's big-ticket data breach complaints is the claim that companies like Wyndham Hotels[36] and TJX,[37] among others, have failed to take reasonably adequate steps to keep information (some sensitive, some not) secure. There is, of course, a legal debate over whether the Federal Trade Commission Act truly authorizes the Commission to take action in security breach cases. The Commission certainly believes so, and a district court recently sided with the Commission in the Wyndham Hotels case.[38] The issue is thus pushing towards resolution; however it is resolved finally, we think the Commission very much should be in the business of protecting consumers from unreasonably dangerous security protocols—and thus far, it has sought to do that.

Finally, it almost goes without saying that the worst forms of consumer exploitation can't be squared with a trusteeship model. And when these have happened, the Commission also has taken swift action. The Path social networking application, for example, knowingly had collected personal information from children under the age of thirteen, without their parents' consent. This violated the Children's Online Privacy Protection Act, as the Commission argued in a subsequent lawsuit.[39] It likewise sued Aaron's, Inc. and DesignerWare, LLC.[40] Some franchisees of the former, a rent-to-own outfit, had installed on their rental computers certain software manufactured by the latter. That software had enabled franchisees to opt—surreptitiously, remotely, and without prior notice to the consumers—for something called "Detective Mode." (The idea was to enable the company to keep tabs on rented items, prevent

34 Complaint, *In the Matter of Myspace LLC*, No. C-4369 ¶¶ 14-16, 21-28 (Aug. 30, 2012).

35 Complaint, *In the Matter of Google, Inc.*, No. C-4336 ¶¶ 7-14 (Oct. 13, 2011); *see also* Complaint for Civil Penalties and Other Relief, *United States v. Google, Inc.*, No. CV12-04177-HRL (N.D. Cal., Aug. 8, 2012) (alleging violation of FTC consent order because, among other things, Google had represented to users of Apple's Safari browser that unless altered, Safari's default settings would preclude the placement of tracking cookies on Safari users' computers; and alleging further that, in fact, Google circumvented the default regime and placed cookies on the computers.); Complaint, *In the Matter of Snapchat, Inc.*, No. 132 3078 ¶¶ 6-45 (May 8, 2014) (alleging that Snapchat engaged in deceptive practices, among other things by falsely representing that users' messages would disappear after the lapse of a set time period).

36 First Amended Complaint for Injunctive and Other Relief, *Federal Trade Commission v. Wyndham Worldwide Corporation et. al.*, No. CV 12-1365-PHX-PGR ¶¶ 24, 47-50 (D. Ariz., Aug. 9, 2012).

37 Complaint, *In the Matter of The TJX Companies, Inc.*, No. C-4227 ¶¶ 8-11 (July 29, 2008)

38 Memorandum Opinion, *Federal Trade Commission v. Wyndham Worldwide Corp. et al.*, No. CV-1887-ES-JAD (D.N.J., April 7, 2014) (denying motion to dismiss).

39 Complaint for Civil Penalties, Permanent Injunction and Other Relief, *United States v. Path, Inc.*, No. C-13-0448 ¶¶ 18-29, 34-48 (N.D. Cal., Jan. 31, 2013).

40 Complaint, *In the Matter of Aaron's, Inc.*, ¶¶ 4-17 (Oct. 22, 2013).

theft, and ensure payment.) Through "Detective Mode," according to legal filings by the Commission, the franchisees "could—and did—secretly gather renters' personal information using fake software registration windows."[41] The franchisees also managed to log renters' keystrokes and to activate the computers' webcams, and accordingly took "pictures of children, individuals not fully clothed, and couples engaged in sexual activities."[42]

The trouble is that the word "privacy" often suggests broader protection—against a wider array of more subjective harms—than the databuse against which the Commission actually enforces. This is, to be sure, not always the case government-wide. Most admirably, the White House's signature privacy proposal, the "Consumer Privacy Bill of Rights," does not overpromise. Though framed in the language of privacy, it does not purport to regulate activity in Category II. As discussed above, this framework document sets out seven norms regarding data collection and use by businesses. The Administration further advocates for the norms' codification, and Commission jurisdiction to enforce them. The White House also envisions a bill that would create an enforcement safe harbor for businesses needing time to align their policies with rules announced in the document; preservation of "sector-specific" privacy statutes; and uniform, nationwide standards for both data protection and security breach notification. In the document's fifty-two pages, you really won't find anything asserting or suggesting that Category II usages are or should be disallowed.

But the White House proposal is perhaps an exception. At times, government officials deploy privacy rhetoric and veer into Category II territory remarkably quickly. The prototypical example of this is the European Union, which is currently considering sweeping privacy regulations that would restrict all sorts of Category II data collection; some proposals even require an affirmative right to be forgotten. U.S. policymakers sometimes have invoked a more expansive vision of privacy, too—and in that respect implied a greater measure of consumer protection than they are likely to deliver.

For example, contrast the Federal Trade Commission's enforcement history with the Commission's rhetoric, which sometimes has a more ambitious sheen than its databuse-oriented actions would lead one to expect. The Commission's posture is complicated here because it has not merely a law enforcement function, but also a long-standing best practices function. Through the latter, the Commission nudges corporations towards a more consumer-friendly stance—even when the corporate behavior in question would give no grounds for enforcement action. Publicly, the Commission has hinted that, in addition to holding databusers to account, it also frowns on some Category II behavior: that which leaves consumers feeling icky or anxious about how their data might be collected or used, even if the corporate action doesn't implicate the obligations of data trusteeship. In this regard, the

41 *Id.* ¶ 4.

42 Complaint, *In the Matter of DesignerWare, LLC et. al.*, No. C-4390 ¶¶ 10-15, 14 (Apr. 11, 2013).

Commission's privacy talk at times has been at little more sweeping in character.

Consider the Commission's preliminary and final reports on consumer privacy ("Preliminary Report," and "Final Report," respectively). Behind these documents was a timely and laudable mission: to figure out how privacy law and policy both ought to be adjusted, given the staggering and near-constant technological advances of the Big Data era. Both drew extensively on staff research, and input from companies, privacy advocates, and other experts. And both broadly concluded that the *status quo* wasn't cutting it. The Preliminary and Final Reports faulted two of the Commission's historical approaches to privacy protection. One was a "notice-and-choice" model, in which the agency would stay its hand provided that a company issued, somewhere, a description of its practices for collecting and using consumer data. The other was the "harm-based model," in which the Commission would sue, in order to shield consumers from certain classes of recognized injuries—all of them of a tangible and objective nature. According to the reports, neither of these rubrics served consumers especially well, in that both allowed Big Data-esque privacy violations to occur. The reports therefore urged industry leaders, Congress, and others to adopt—through an admixture of legislation and best practices—a new "framework" for safeguarding privacy.

The Preliminary Report sketched out a more capacious and fuzzier privacy vision than anything the Commission had previously articulated. In one section, it criticized the harm-based model as cramped and outdated, among other things because that regime appeared not to account for consumers' anxieties about Big Data's ominous side effects:

> The FTC's harm-based approach also has limitations. In general, it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy related harms is much wider and includes reputational harm, as well *as the fear of being monitored or simply having private information "out there."* Consumers may feel harmed when their personal information—particularly sensitive health or financial information—is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations.[43]

Note the italics. How much power did the Commission really have, to bring legal cases founded on subjective fears and the like? In the view of then-Commissioner Thomas Rosch, the answer was straightforward: none. According to Rosch, "the Commission could overstep its bounds if it were to begin considering "the fear of being monitored" or "other intangible privacy interests generally when analyzing consumer injury."[44] Rosch wrote in a statement concurring in the Preliminary Report that "[t]he Commission has specifically advised Congress that absent

43 FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: a Proposed Framework for Businesses and Policymakers at 20 (2010) ("Preliminary Report") (emphasis added).

44 Preliminary Report, Concurring Statement of Commissioner Thomas Rosch at E-5.

deception, it will not enforce Section 5 [of the Federal Trade Commission Act] against alleged intangible harm."[45] He here referred to two "policy statements," in which the Commission, in the 1980s, had set forth its understanding of just how far it could go in deeming corporate practices to be "unfair" or "deceptive." In particular, the Commission had declared that "[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair."[46] Rosch thus seemed to wrestle with what the Preliminary Report so strongly implied: that the Commission's new thinking regarding the parameters of privacy harm might also portend a novel application of consumer protection law.

The 2012 Final Report did not take on Rosch's critique explicitly. But it did appear to double down on the Preliminary Report's conception of privacy harm:

> The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties.[47]

This formulation was also vague enough to raise Rosch's eyebrow, and for the same reasons as before. Elsewhere, the Final Report had discussed a complaint brought against Google on the basis of deception—a posture that typically does not require proof of tangible harm, but instead, a material misrepresentation to consumers.[48] Referring to that case, the Commission said "a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions." But, as Rosch pointed out, an explanatory footnote to that sentence also hinted that, under the Commission's new privacy framework, the Commission might have intervened *even if the company had not acted deceptively*. "[E]ven in the absence of . . . misrepresentations," said the Final Report, "revealing previously-private consumer data could cause consumer harm."[49] To Rosch's eye,

45 *Id.; see also* Preliminary Report, Concurring Statement of Commissioner William Kovacik at D-2 (noting that Preliminary Report "differs from earlier reports, though, in proposing an expanded concept of harm (although [the Preliminary Report] does not address how the Commission's application of the harm test has developed in practice).")(footnote omitted).

46 Unfairness Policy Statement at 3.

47 FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 8 (2012) ("Final Report"); *see also id*. at 2 & n. 5 (noting that participants in discussions held between Preliminary and Final Reports criticized the "harm-based" model, among other things because it failed "to recognize a wider range of privacy-related concerns, including … fear of being monitored.").

48 Final Report, Dissenting Statement of Commissioner J. Thomas Rosch at C-8 & n. 42.

49 *Id*.

all this "broadly hint[ed]" that a failure to heed the Commission's framework might give rise to a legal complaint founded on a new theory of the Commission's authority.[50] The Final Report had claimed to the contrary, insisting that, to the extent the recommendations surpassed the obligations imposed by existing law, its recommendations were just that: recommendations.[51]

As we have noted, the Commission's enforcement history is broadly consistent with a databuse approach. So the more expansive vision in the Final Report is best understood as a push on the best practices front, not a claim of power under the law. Still, the fact that a member of the Commission itself was unclear about exactly what the Commission was saying about the scope of its authority has to be significant. And controversy over the Final Report's significance has persisted. One of Rosch's successors, Commissioner Maureen Ohlhausen, echoed him in both congressional testimony and public statements. She expressed "reservations" about the Final Report's seeming "embrace [of] an expansion of the definition of harm to include 'reputational harm,' or 'the fear of being monitored,' or 'other intangible privacy interests.'"[52]

CONCLUSION

Consumers, governments and companies need more guidance than the broad concept of privacy—which incorporates such a huge range of potential obligations—often can meaningfully furnish. As a narrowing subset, databuse does a better job of portraying the government's current consumer protection efforts and legislative ambitions. In that respect, it offers all parties a firmer sense of what sorts of data uses actually are and are not off-limits. That's to the good, given that everyone wants greater clarity about the protections consumers actually require—and actually can expect—as against companies that ingest data constantly and by the boatload.

That's the difficulty with vague privacy talk, when it disparages data usages by companies that don't measurably harm the companies' customers. The Preliminary Report saw privacy harm in the "fear of being monitored." But the Commission doesn't sue companies simply because they stir those fears, and the Commission really isn't asking for statutory power to do so, either. Nor is the White House, in its proposal for a Consumer Privacy Bill of Rights—which, again, largely recommends policies that jibe with our approach.

---

50 *Id*.

51 Final Report at iii ("To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.")

52 Statement of FTC Commissioner Maureen K. Ohlhausen, "The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing Before the Senate Committee on Commerce, Science, and Transportation at 2 (May 9, 2012); *see also e.g.* FTC Commissioner Maureen K. Ohlhausen, "The Government's Role in Privacy: Getting It Right," Hudson Institute at 2-3 (Oct. 16, 2012) (noting that Final Report "did appear to embrace an expansion of the concept of harm to include reputational or other intangible privacy interests" not previously recognized under Commission interpretations of the "unfairness" prong of Section 5 of the Federal Trade Commission Act).

By observing that databuse better describes the government's behavior and short-term aspirations for consumer protection, we do not mean to proclaim the current setup to be optimal, or to counsel against further legislation. To the extent current law is not yet framed in terms of databuse—and it is not—the protections the Commission has quite reasonably grafted onto the unfair and deceptive trade practice prohibitions of the Federal Trade Commission Act should probably be fixed in statute. And if Congress wants to go further, it should raise standards, too, by more uniformly requiring the sorts of practices we hold out as models of good trusteeship above. The best example here is data security; the obligation to provide it, on pain of Commission enforcement, has only recently (and somewhat tenuously) been accepted by the judiciary. Congress should take things a step further, by making clear, and standardized, the obligation of all companies to take all reasonable measures to keep data secure, and to notify consumers promptly about security breaches. To put the point differently, we need a statute of the type the Commission and the White House both have called for.[53]

But what the government should *not* do is to push past databuse's conceptual boundaries, and step into a more subjectively-flavored, loosely-defined privacy enforcement arena. We do not make law to defend "democracy" in its broadest sense; we subdivide that umbrella value into campaign finance law, redistricting, and other more manageably narrow ideas. The same holds true for "privacy"—which, as a concept, is simply too gauzy, too disputed to serve as a practical guide. As its most fervent advocates understand it, it is a concept that might actually protect consumers far more than they wish to be protected. The costs of a sweeping "privacy" approach may well be to stifle and impede the delivery of services large numbers of people actually want. But isolating the core we actually mean to guarantee is one way of guaranteeing that core more rigorously.

53 *See, e.g.,* Final Report at i, 12 & n. 65 (citing the Commission's past calls for the enactment of data security legislation).

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
brookings.edu/governance.aspx

Editors
Christine Jacobs
Beth Stone

Production & Layout
Beth Stone

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU