ABOUT THE AUTHORS


Wells C. Bennett is a Fellow in the Brookings Institution’s Governance Studies program, and Managing Editor of Lawfare, a leading web resource for rigorous, non-ideological analysis of “Hard National Security Choices.” He concentrates on issues at the intersection of law and national security, including the detention and trial of suspected terrorists, targeted killing, privacy, domestic drones, Big Data, and surveillance.
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 handling 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 that company or government ought to handle that data.

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, in a paper entitled “Database: Digital Privacy and the Mosaic,” 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 “database,” 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.”

Database, the paper argued, “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 attempt in this essay to sketch out the data protection obligations that businesses owe to their users. 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.

The values and duties that make up this consensus 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 used; 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 database.

And we argue that protection against database—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.

Privacy, Trusteeship, And Database
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. The word promises a great deal more than policymakers are prepared to deliver, and in some ways, it also promises more than consumers want.

The concept certainly was not inevitable as the reference point for discussions of individual rights in the handling of data. It developed over time, in response to the obsolescence of previous legal constructions designed to shield individuals from government and one another. To put the matter simply, 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.

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. 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 with more hostility.
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. 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. Database 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.² It instead treats the dissemination of such data—in whole or in part—as an option we might or might not want to choose.

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 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.³ A trustee is bound to act prudently, with reasonable care, skill, and caution,⁴ and to keep beneficiaries reasonably informed, both about the trust’s formation and its subsequent activities—including any changes to the trust’s operation.⁵

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. The essence of this sort of data trusteeship 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. These components 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.” In the years since, scores of articles, privacy policies, and government documents have drawn on the FIPPs. 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.⁶ 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 show, they also reflect the set of expectations that, when companies fail to meet them, yield enforcement actions by the Federal Trade Commission (FTC). And they also reflect the commitments the major data-handling companies
actually make to their users. In other words, the components of database are the parts of privacy about which we all basically agree.

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 actually providing data only to those entities to which he or she actually agrees to give them. 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.

Second, companies must never use consumer data in a fashion prejudicial to the interests of consumers. Consumers are far savvier 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 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. 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: 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. Rather, it means 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, for instance, have both created 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. 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. Google offers users remarkably granular control over what sort of advertising they do and don’t want to see and to what extent they want advertising based on their recorded interests. The more control consumers have over who has

“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.”
access to their data and what the trustee company can do with it, 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. Promising a whole lot of user control is worthless if the promises are not honored. And a great many of the FTC’s enforcement actions naturally involve allegations of companies committing themselves to a set of practices and then failing to live up to them. Notice how much of conventional privacy this conception leaves out. For starters, it leaves out 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 FTC 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 this out. 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.

**Interests Congruent And Conflicting**

One simple way to think about the spectrum between good trusteeship and databuse is to examine the similarity 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. 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 perversely 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 fastest travel routes from one place to another while avoiding 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 utilized and its contents electronically repackage 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 while avoiding 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 utilized and its contents electronically repackage 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. 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 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. Category I data 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 generally does not raise the hackles of privacy advocates, and the pure Category I situation generally ought to draw the most minimal attention from policymakers, as well as 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.\textsuperscript{13}

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. That said, we think as a general matter that advertising does not fit into Category I. Some 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.

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 or the other. But in and of themselves, the ads neither advantage him nor do him harm.

Category II uses often bother some privacy activists. 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. 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.

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. But seen through a more modest database lens, these are relationships into which a reasonable consumer might responsibly choose to enter 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, database, 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. Previously, we explained that database is the “right to not have your data rise up and attack you.” 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 punished 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 using 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. Trusteeship is normative in that it is designed to ensure a beneficiary’s confidence and create conditions for the beneficiary’s success. Market principles are ambivalent and thus suggest a just-do-the-least-required-to-further-one’s-own-
ends sort of regime. A pure market approach would tolerate, for example, a minimally adequate corporate policy about how data is collected, used, and disseminated, or it would 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 generous 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.\textsuperscript{18}

The same idea holds true in other areas relevant to the two-sided arrangement between the person contributing data and the company holding data. The market might only require the company 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 and instead will require additional consent for uses beyond those reasonably or necessarily following from the nature of the consumer's transaction with the company.\textsuperscript{19}

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 FTC 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.\textsuperscript{20} 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.

**Conclusion**

Consumers, governments, and companies need more guidance than the broad concept of privacy 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—it disparages data usages by companies that don’t measurably harm the companies’ customers. The FTC doesn’t sue companies simply because they stir 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.

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

\textbf{“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.”}
extent current law is not yet framed in terms of databuse—and it is not—the protections the FTC 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.

But what the government should not do is 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.

ENDNOTES


2 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, 30 Nov. 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, 12 Feb. 2013, describing early-stage efforts by companies to permit consumers to profit from data sales.

3 Restatement (Third) of Trusts § 78.

4 Ibid., § 77.

5 Ibid., § 82.


8 See, “Consumer Data Privacy,” 14, recommending consumer “right to easily understandable and accessible information about privacy and security practices”; “Protecting Consumer Privacy,” 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,” 30, arguing that information disclosed to consumers regarding companies’ data practices should be “accessible, clear, meaningful, salient and comprehensible to its intended audience.”

9 See, “Consumer Data Privacy,” 11, recommending consumer “right to exercise control over what personal data companies collect from them and how they use it”; “Protecting Consumer Privacy,” 1, 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,” 69, “A key goal is to protect informed choice and to safeguard the ability of consumers to control access to personal information.”

ENDNOTES CONTINUED


13 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,” Washington Law Review, 79, no. 119 (2004); Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (Stanford Law Books, 2010); see also, “Consumer Data Privacy,” 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; “Protecting Consumer Privacy,” 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,” 18 and n. 11, “A wide variety of authorities recognize that information privacy depends on context and that expectations of privacy in the commercial context evolve.”

14 Jon Healey, “Privacy Advocates Attack Gmail – Again – for Email Scanning,” The Los Angeles Times, 15 Aug. 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; “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.

15 See Footnote 13.


18 See Footnote 8.

19 See Footnote 13.

20 “Protecting Consumer Privacy,” 9 and n. 40, noting, among other things, comments from Google regarding its subscribers, who use Google’s Ads Preference Manager and remain “opted in.”