Berkeley Technology Law Journal

Volume 33 | Issue 1 Article 1

6-23-2018

Information Fiduciaries in Practice: Data Privacy and User Expectations

Ariel Dobkin
Yale Law School

Link to publisher version (DOI)
https://doi.org/10.15779/Z38G44HQ81

Information Fiduciaries in Practice: Data Privacy and User Expectations

Cover Page Footnote
The author would like to thank Jack Balkin for his thoughtful suggestions and support throughout many stages of this Article. She also thanks James Durling, Jackie Koo, Hilary Ledwell, Jenna Pavelec, Alexandra Perloff-Giles, and Jacobus van der Ven for their invaluable input at various phases of this Article's production. Finally, the author is grateful to Bihter Ozedirne, Charles Miller, and Alice Chi, as well as Christian Chessman and the editors at the Berkeley Technology Law Journal, for their careful editing and hard work on this Article.

INFORMATION FIDUCIARIES IN PRACTICE: DATA PRIVACY AND USER EXPECTATIONS

Ariel Dobkin†

ABSTRACT

Every day, consumers give their personal information to corporations in exchange for free or inexpensive services. As service providers collect increasingly personal information, they will not be able to use it just to inform business decisions, but also to manipulate users, push agendas, or discriminate surreptitiously. And users may not know exactly how these companies collect and use their data, so they may not be equipped to respond effectively to objectionable data collection practices. The law does nothing to manage this relationship, and in fact, the Supreme Court has interpreted the First Amendment to prevent certain regulation of data collection or usage. However, imposing an information fiduciary duty on service providers could ensure that they use data only in ways that are consistent with users' expectations. This Article maintains that service providers should be proscribed from utilizing users' personal information to manipulate them and discriminate against them, and that firms should be prohibited from sharing data with third parties under certain circumstances. It also proposes that firms engage with their users by employing easy-to-understand privacy policies that help reduce information asymmetries. Ultimately, imposing an information fiduciary duty on service providers can ensure that firms are able to grow and innovate and that their users—whose data is necessary for that growth—are protected as well.

DOI: https://doi.org/10.15779/Z38G44HQ81

† Yale Law School, J.D. 2017. The author would like to thank Jack Balkin for his thoughtful suggestions and support throughout many stages of this Article. She also thanks James Durling, Jackie Koo, Hilary Ledwell, Jenna Pavelec, Alexandra Perloff-Giles, and Jacobus van der Ven for their invaluable input at various phases of this Article's production. Finally, the author is grateful to Bihter Ozedirne, Charles Miller, and Alice Chi, as well as Christian Chessman and the editors at the *Berkeley Technology Law Journal*, for their careful editing and hard work on this Article.

TABLE OF CONTENTS

> "It's the little things that reveal what a company is all about at its core. . . . A great, long-lived brand begins and ends with trust."
>
> —Peter Sims, whose data was displayed publicly at an Uber launch party[1]

I. INTRODUCTION

Imagine riding in an Uber car and receiving a phone call from a friend in another city. When you pick up, she recites your location to you. When you turn a corner, she knows where you are. When you have arrived at your destination, she knows that too. Or imagine being a girl in high school and your father finding out you are pregnant because Target sent you coupons for maternity clothes. Or feeling more depressed over the last week, only to find out that over the same time period, Facebook performed an experiment to tinker with its users' emotions.

Real people have found themselves in each of these situations over the past several years. Peter Sims, an entrepreneur in New York, found himself in the first situation in 2014, when Uber displayed his location on a wall at its Chicago launch party.[2] A young girl in Minneapolis found herself in the second situation several years earlier.[3] And Facebook did in fact perform an experiment to "manipulate[] the news feeds of over half a million randomly selected users to change the number of positive and negative posts they saw, [as] part of a psychological study to examine how emotions can be spread on social media."[4] In each situation, a company took advantage of personal information it possessed—information with which users had entrusted them—for its own benefit. The service providers used that data in a way that likely breached the trust that Peter Sims, the young girl, and half a million others had placed in them. In none of these situations, fortunately, did a report of harm surface, but the potential was not far off. Imagine if Mr. Sims had a dangerous stalker, if the Minneapolis teenager had an abusive parent, or if a depressed Facebook user had been pushed far enough to commit suicide. The

1. Peter Sims, *Can We Trust Uber?*, SILICON GUILD (Sept. 26, 2014), https://thoughts.siliconguild.com/can-we-trust-uber-c0e793deda36 [https://perma.cc/L7JB-GTDY].

2. *Id.*

3. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/R3D6-HSLN].

4. Vindu Goel, *Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (June 29, 2014), www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html [https://perma.cc/CL49-GNWK].

companies' efforts to boost their profits took precedence over protecting the sensitive and private information of their users.

Every day, users knowingly and unknowingly trade their data—often instead of their money—for goods and services with companies that profit off of their personal information.[5] In fact, at least 77.4% of websites globally track visitors' data.[6] Users may on some level realize that their data is valuable, but they may not think twice before handing it over to service providers; those who do consider it may still prefer paying with data to paying with money.[7] This behavior by both groups of people is a manifestation of their trust in these companies. Even as users may be unable to articulate exactly how service providers should and should not use their data, they have implicit expectations. We each have a gut reaction that tells us when a company has crossed the line: we may have no problem when Uber remembers our home address so that we can avoid typing it in every time we use the service, but we would feel that our privacy had been violated if Uber were to provide a database through which anyone could look up our rider histories. Few people mind that Facebook shows them targeted advertisements,[8] but many might react negatively if Facebook began selling access to their Facebook profiles to potential employers or landlords. Users' expectations and tolerance differ at the margins,

5. *See* ANNA BERNASEK & D.T. MONGAN, ALL YOU CAN PAY: HOW COMPANIES USE OUR DATA TO EMPTY OUR WALLETS 208 (2015); *see also* David B. Kline, *How Does Google Make Money? Ads, Ads, Ads*, MOTLEY FOOL (June 14, 2015, 11:31 AM), https://www.fool.com/investing/general/2015/06/14/how-does-google-make-money-ads-ads-ads.aspx [https://perma.cc/UX7Y-REA8] (explaining that 90% of Google's revenue in 2015 came from advertising); Tim Wu, *Facebook Should Pay All of Us*, NEW YORKER (Aug. 14, 2015), http://www.newyorker.com/business/currency/facebook-should-pay-all-of-us [https://perma.cc/N5JH-8YBL] ("The two-hundred-and-seventy-billion-dollar valuation of Facebook, which made a profit of three billion dollars [in 2014], is based on some faith that piling up all of that data has value in and of itself. It's like a virtual Fort Knox—with a gold mine attached to it.").

6. Sam Macbeth, *Tracking the Trackers: Analysing the Global Tracking Landscape with GhostRank*, GHOSTERY (July 2017), https://www.ghostery.com/lp/study [https://perma.cc/27EC-R5J8] (describing a study of 850,000 users and 144 million page loads in more than twelve countries).

7. The Digital Advertising Alliance, for example, found that 58% of adults who download phone apps "preferred free, ad-supported apps to those that required some form of payment . . . ." Greg Sterling, *Survey: 58 Percent Prefer Ad-Based Apps to Paid, Freemium Models*, MARKETING LAND (Oct. 26, 2014, 11:31 AM), http://marketingland.com/survey-proclaims-consumer-preference-ad-supported-apps-daa-readies-mobile-appchoices-105463 [https://perma.cc/V9LN-KXAZ].

8. David Kirkpatrick, *Study: 71% of Consumers Prefer Personalized Ads*, MARKETING DIVE (May 9, 2016), http://www.marketingdive.com/news/study-71-of-consumers-prefer-personalized-ads/418831 [https://perma.cc/K3RA-MTBG].

but certain practices would likely be widely regarded as having crossed a line. And it is important for service providers to maintain users' trust, which "can evaporate in an instant if customers feel their data is being used improperly, or not effectively protected."[9]

But the threat of trust disappearing is not enough to influence service providers to protect user privacy on their own. Because users often do not know or understand how their data is being used, the market cannot simply "work its magic" and encourage best privacy practices; markets rely on consumers having enough knowledge to inform their decision-making.[10] When consumers lack information, they cannot respond to company practices effectively enough to affect the market. And thus, too often, companies are able to cross the line into data usages many users would oppose, because the users never know about it.[11]

Companies readily acknowledge that they are not transparent about their data usage. In January 2016, *The Economist*'s Intelligence Unit released the results of a study demonstrating that almost sixty percent of professionals surveyed globally are "generating revenue from the data they own and will continue to do so," and eighty-three percent say it makes "existing products or services more profitable."[12] But only thirty-four percent of those surveyed believe that "their firms are 'very effective' at being transparent with customers about how they use their data," while nine percent "admit to being 'somewhat' or 'totally ineffective.'"[13] Despite this admitted lack of transparency, the U.S. government does not adequately regulate service providers in any comprehensive way.

---

9. Bernard Marr, *Big Data Facts: How Many Companies Are Really Making Money from Their Data?*, FORBES (Jan. 13, 2016, 2:24 AM), www.forbes.com/sites/bernardmarr/2016/01/13/big-data-60-of-companies-are-making-money-from-it-are-you/ [https://perma.cc/NNC7-8642].

10. *See* Ryan Bubb & Richard H. Pildes, *How Behavioral Economics Trims Its Sails and Why*, 127 HARV. L. REV. 1593, 1601, 1639 (2014) (discussing information asymmetry as a reason for market failure); Brendan A. Cappiello, The Price of Inequality *and the 2005 Bankruptcy Abuse Prevention and Consumer Protection Act*, 17 N.C. BANKING INST. 401, 429 (2013) ("[M]arkets, especially financial markets, require the buyer and seller to have similar knowledge about the transaction in order for it to function properly."); Justin M. Ross, *What Should Policy Makers Know When Economists Say 'Market' Failure?*, 14 GEO. PUB. POL'Y REV. 27, 28 (2009) (noting that "information problems" are a "common source" of market failure).

11. *See, e.g.*, *supra* notes 2–4 and accompanying text.

12. *The Business of Data*, ECONOMIST 7, 10 (2015), www.eiuperspectives.economist.com/sites/default/files/Business%20of%20Data%20briefing%20paper%20WEB.pdf [https://perma.cc/ERN9-U8CX]; *see also* Marr, *supra* note 9.

13. ECONOMIST, *supra* note 12, at 4, 12.

Companies are committed to keeping it that way. Walmart, for example, spent almost $34 million on lobbying over five years "on some variation of 'privacy, online advertising and data protection,' 'privacy and online behavioral advertising legislation,' or 'privacy issues related to e-commerce.'"[14] And that was during a period in which Congress was not pushing to regulate data collection in the first place. The laws that currently exist to protect individuals' data focus on specific subject matters or populations, rather than establishing a minimum level of protection across the board. For instance, federal laws exist to protect children's data[15] and to regulate data usage in particular fields.[16] Additionally, federal agencies have sued companies for violating their own privacy policies.[17] The Obama Administration published white papers on data privacy that recognized the need for better protections, but it never suggested a comprehensive solution.[18]

More problematically, a 2011 Supreme Court decision, *Sorrell v. IMS Health*,[19] indicates that in at least some circumstances, the First Amendment protects the sale of data by private firms. There, the Court struck down a Vermont statute restricting the sale, transmission, or use of pharmaceutical data, after subjecting it to heightened scrutiny.[20] This decision complicated the possibility of data privacy regulation by bringing at least some data sharing within the protection of the First Amendment.

Thus, the current state of the law not only fails to protect the average user, but also indicates that regulating the way data is used or shared may be unconstitutional under the First Amendment. The government can certainly regulate little pockets that may withstand heightened scrutiny, but absent some

14. CTR. FOR MEDIA JUSTICE ET AL., CONSUMERS, BIG DATA, AND ONLINE TRACKING IN THE RETAIL INDUSTRY: A CASE STUDY OF WALMART 14 (2013), http://centerformediajustice.org/wp-content/uploads/2014/06/WALMART_PRIVACY_.pdf [https://perma.cc/7UVT-MWPQ].

15. *See, e.g.*, Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312 (2013).

16. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; Truth in Lending Act, 15 U.S.C. § 1601 (2012).

17. *See, e.g.*, *Privacy & Data Security Update (2015)*, FED. TRADE COMM'N (Jan. 2016), www.ftc.gov/reports/privacy-data-security-update-2015 [https://perma.cc/ZW9S-ZBYN] (summarizing FTC enforcement actions including "over 130 spam and spyware cases and more than 50 general privacy lawsuits").

18. *See, e.g.*, WHITE HOUSE, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf [https://perma.cc/ZY36-LXFY] (calling attention to the importance of data privacy without proposing any concrete paths forward).

19. 564 U.S. 552, 557 (2011).

20. *Id.*

countervailing theory, the United States is currently unable to grapple with the challenges that lie ahead. While defending freedom of speech is vital, so is protecting consumers' privacy during a time in which companies know more about us than users' friends or families might. The use of personal information by private firms—to advertise, to build artificial intelligence, to shape public opinion, and more—presents incredible opportunities and benefits to society, as well as disturbing possibilities for manipulation and discrimination. In order to manage these challenges, it is necessary to find a way to protect users without interfering with service providers' First Amendment rights.

Conceiving of service providers as "information fiduciaries" may be the way to balance freedom of speech with data privacy, while still allowing service providers to grow and innovate. As designated information fiduciaries, service providers would have "special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[21] Jack Balkin explains that "in the digital age, because we trust them with sensitive information, certain types of online service providers take on fiduciary responsibilities."[22] In his article, Balkin suggests imposing a general fiduciary duty on service providers who collect or use data, and he reconciles the First Amendment concerns espoused in *Sorrell* with the public's need for increased regulation of data collection and usage by companies.[23] The article argues convincingly for an information fiduciary duty in theory, but the next step is to determine what that duty will look like in practice.

Thus, this Article extends that work by attempting to determine where the line is—what are the things that consumers, as a collective, trust companies *not* to do, and with what practices *are* consumers comfortable? How can policymakers develop an information fiduciary duty that is in line with users' expectations? Ultimately, this Article argues that companies breach the fiduciary duty when they abuse users' trust by: (1) using their data to manipulate them; (2) using their data to discriminate against them; (3) sharing their data with third parties without consent; or (4) violating their own privacy policies. After describing each principle in theory, this Article presents a set of hypotheticals to make the implications of each more concrete. By examining how various fact patterns would interact with the fiduciary duty for the service provider in question, this Article begins to visualize the duty in a way that makes it a practical legal possibility. In these hypotheticals—many of which are inspired by true events—this Article utilizes a set of companies to

21. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016).

22. *Id.* at 1221.

23. The First Amendment is less likely to tolerate the sharing of information about a person to whom you owe a duty of trust and confidence with respect to that information.

determine how an information fiduciary standard might be applied in practice: Walmart, Uber, Facebook, and Google. Although the information fiduciary framework will allow many companies to continue their current practices involving data collection, retention, or usage, the hope is that it will simultaneously prevent unexpected and abusive practices. Finally, the Article closes with a short discussion of what would be necessary to make the information fiduciary duty a legal reality.

II. BACKGROUND

Because this theory—and indeed, this field—is so new, this first Part aims to provide necessary background information, laying the groundwork for a theoretical information fiduciary duty. It first briefly outlines various privacy regimes that do exist and explains their failure to adequately protect the average user's privacy. Then, it summarizes Jack Balkin's proposal for an informational fiduciary duty, which, with the proper contours, may be able to fill this gap. Finally, this Part describes the data collection practices of four well-known companies to illustrate common data collection and usage capabilities.

A. EXISTING PRIVACY REGIMES

American law sparsely regulates the ways in which private firms collect and utilize users' data. The categories of regulation fall into two camps: (1) laws that protect privacy for certain groups of people or certain kinds of data, and (2) enforcement actions by the Federal Trade Commission (FTC) and other agencies as they apply relatively broad mandates to Big Data and its ramifications.[24] Although these mechanisms are certainly better than nothing, they allow the typical service provider to utilize data in many objectionable ways. They are inadequate protections on their own.

The United States Congress has passed several statutes regulating data usage.[25] However, there is no sweeping standard for how private firms treat data; each law is tied to a specific subject area or protects a certain class of citizens. For example, the Health Insurance Portability and Accountability Act (HIPAA) regulates how healthcare organizations must secure electronic

24. Of course, there are other laws that regulate the way the United States government can collect and use its citizens' data. Those laws—and their adequacy—are outside the scope of this Article. Similarly, the United States-European Privacy Shield affects how U.S. businesses can interact with the data of European citizens, but because it does not protect American users, it is similarly outside the scope of this Article.

25. *See, e.g.*, Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-6 (2012); Children's Online Privacy and Protection Rule, 16 C.F.R. pt. 312 (2013).

medical records and, thus, patients' privacy.[26] Although it protects all users, it covers only their health data. On the other hand, the Children's Online Privacy and Protection Rule (COPPA), a regulation promulgated by the FTC, covers many categories of data but protects only users under the age of thirteen.[27] Congress has not yet attempted to establish a general data regime that regulates private firms in this space.

At present, the only protection users have is the privacy policies that service providers design and implement themselves, and there is no baseline protection to fall back on if they withdraw or weaken these policies. But at least the FTC and other agencies do have the power to hold companies to their own promises. Through enforcement and the threat of enforcement, the FTC ensures firms do not utilize "unfair" or "deceptive" practices, and it has sought consent decrees against service providers who violate their own privacy policies.[28] For example, in June 2016, the FTC fined an advertising company $950,000 for violating its own privacy policy. The company represented to users that it "would only track consumers' locations when they opted in and in a manner consistent with their device's privacy settings."[29] In fact, however, InMobi tracked hundreds of millions of users' geolocation data without their consent, even when they had turned off location tracking on their phones.[30] Similarly, the Consumer Financial Protection Bureau (CFPB), which is charged with preventing deceptive, unfair, and abusive practices in the consumer financial services space,[31] fined an online payment platform $100,000 for advertising that its security protection exceeded industry standards while the "data security practices in fact fell far short of its claims."[32]

But enforcing companies' own standards is not enough. Firms should not be able to dictate the standards to which they hold themselves—and regulators would not have power over a company that violates its users' privacy unless it

26. 42 U.S.C. § 1320d-6 (2012); *see also Notice of Privacy Practices*, U.S. DEP'T HEALTH & HUMAN SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html [https://perma.cc/K399-2EP7].

27. 16 C.F.R. §§ 312.2–12.3 (2017).

28. *See* 15 U.S.C. § 45 (2012).

29. Press Release, Fed. Trade Comm'n, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked [https://perma.cc/E2D3-UP4J].

30. *Id.*

31. 12 U.S.C. § 5531 (2012).

32. Press Release, Consumer Fin. Prot. Bureau, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices [https://perma.cc/9UDU-K9NX].

also violated its own policy. That means service providers have an easy out: implement a very broad privacy policy that it is difficult to violate. As the next Section explains, an information fiduciary duty would require a minimum level of protection regardless of the privacy promises companies make on their own.

B. AN INFORMATION FIDUCIARY DUTY

Definitions of a fiduciary vary, but it has been described by one court as:

> [T]he acting of one person for another; the having and the exercising of influence over one person by another; the reposing of confidence by one person in another; the dominance of one person by another; the inequality of the parties; and the dependence of one person upon another. In addition, courts have considered . . . knowledge of the facts involved or other conditions giving to one an advantage over the other.[33]

As the American Bar Association (ABA) states, "[w]henever one party places trust and confidence in a second person with that second person's knowledge, it is possible that a fiduciary relationship is created."[34] In other words, fiduciary law "assume[s] that professionals and their clients do not stand on an equal footing."[35] As a result, a fiduciary has a legal obligation to act in the best interests of her clients because the clients depend on the fiduciary.[36] This dynamic exists in various industries in many forms. For example, physicians must act in their patients' best interests and attorneys must act in their clients' best interests.[37] All of these relationships have a common dynamic: there is an information asymmetry, so both parties know that the person with less information will trust or rely on the person with more information. To manage this dependency, the law imposes a special duty on the person with more information to ensure that she does not take advantage of the asymmetry.

Jack Balkin argues that service providers who collect and utilize user data are fiduciaries "in the digital age, because we trust [service providers] with

33. Robert A. Kutcher, *Breach of Fiduciary Duties*, *in* BUSINESS TORTS LITIGATION 1, 3 (David A. Soley, Robert Y. Gwin & Ann E. Georgehead eds., 2d ed. 2005) (quoting First Bank of Wakeeney v. Moden, 681 P.2d 11, 13 (Kan. 1984)).

34. *Id.*

35. Balkin, *supra* note 21, at 1216.

36. *See* Kutcher, *supra* note 33, at 3. A related idea exists in contract law, which protects buyers who rely on a seller's special expertise through an implied warranty of fitness for a particular purpose. U.C.C. § 2-315 (AM. LAW INST. & UNIF. LAW COMM'N 2012).

37. While not all of these relationships are known as "fiduciary" relationships, the dynamic itself exists within all of them. The author uses the term "fiduciary" for ease of understanding.

sensitive information."[38] As he explains, end-users are vulnerable to these companies but dependent on them, while service providers are experts on their own data collection and usage practices. And because of this, "information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[39]

This is a point with enormous consequences: because users trust service providers with their information, the law should impose a duty to protect the users. But agreeing that providers owe a "fiduciary duty" is only the first step. The next move is to determine what the duty looks like: which practices may service providers implement consistent with their duty, and which must they avoid? In listing the "literally hundreds of ways in which [general] fiduciaries may breach [their] duties," the ABA includes failure to act in another's best interest, misuse of confidential information, misuse of superior knowledge or position, failure to disclose, and misappropriation of property.[40] All of these breaches stem from an understanding that when two parties engage in a fiduciary relationship, the inferior party gives the superior party power to help it make decisions, and thus trusts it to do so in a way that does not harm the inferior party.

The trust users place in service providers "impl[ies] an expectation of predictability."[41] Users trust businesses with their data and that trust may be broken when companies use it in a way that users could not have predicted. Put another way, when users' expectations are disregarded by service providers, their trust may be violated. But of course, the confidence people have in a firm they trust often "outstrips [their] knowledge" of what that firm actually does.[42] So users often misplace their trust and subject themselves to wholly unexpected consequences. But from a market perspective, it is vital for a business to maintain its customers' trust. In the online space, for example, studies have shown that "consumers prefer to do business with Web sites that

38. Balkin, *supra* note 21, at 1221.

39. *Id.* at 1186. Furthermore, this point addresses the concern that when service providers use or sell data, they are engaging in activity protected by the First Amendment. While the Supreme Court has held that a statute banning the sale, transmission, or use of data by pharmacies, health insurers, and similar entities is an unconstitutional restriction of their right to free speech, *see* Sorrell v. IMS Health, 564 U.S. 552 (2011), imposing an informational fiduciary standard on service providers circumvents this problem. Because a fiduciary relationship has an elevated status, the service provider would have less freedom under the First Amendment than other speakers. Balkin, *supra* note 21, at 1209.

40. Kutcher, *supra* note 33, at 11.

41. ROBERT C. SOLOMON & FERNANDO FLORES, BUILDING TRUST: IN BUSINESS, POLITICS, RELATIONSHIPS, AND LIFE 71 (2001).

42. *Id.*

they perceive to be reliable, honest, consistent, competent, fair, responsible, helpful, and altruistic—key components of trust."[43]

But *how* do users trust companies to protect their data, and what uses of their data would they oppose if they knew about it? What can users reasonably expect, and what practices would be unpredictable and inconsistent with the duty? Balkin provides a number of general principles to define the information fiduciary duty, such as the idea that a company is an information fiduciary "when the affected individuals reasonably believe that [it] will not disclose or misuse their personal information based on existing social norms of reasonable behavior, existing patterns of practice, or other objective factors that reasonably justify their trust."[44] More detail is needed to visualize the information fiduciary duty as something that can be implemented in practice.

C. HOW FOUR COMPANIES UTILIZE USER DATA

In order to understand what users can reasonably expect from service providers, it is helpful to be aware of firms' capabilities. This Section briefly describes the data capabilities of four companies: Walmart, Uber, Facebook, and Google. These firms serve as the basis for many of this Article's hypotheticals.[45] Each company has a meaningful amount of public information about its data practices, sometimes through its own doing and other times through the work of investigative journalists and others. Each also serves as a representative of its broader industry.

1. Walmart

Every hour, Walmart takes in two and a half petabytes—the equivalent of 167 times the books in the Library of Congress—of "unstructured data" from one million customers.[46] This data covers 145 million Americans, or more than sixty percent of American adults.[47] Walmart and other big-box stores have access to consumer data including names, contact information (email addresses, physical addresses, and phone numbers), and purchase histories.

43. Miriam J. Metzger, *Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce*, 9 J. COMPUTER-MEDIATED COMM. 00 (2004).

44. Balkin, *supra* note 21, at 1224.

45. This Article deliberately avoids service providers in the health or financial industries. While these areas certainly present a host of important privacy questions, they are already subject to a number of regulations that could distract from a pure analysis of information fiduciary duties.

46. *How Big Data Analysis Helped Increase Walmarts Sales Turnover?*, DEZYRE (Nov. 10 2017), https://www.dezyre.com/article/how-big-data-analysis-helped-increase-walmarts-sales-turnover/109 [https://perma.cc/XGV4-XAVS].

47. *Id.*; *see also* CTR. FOR MEDIA JUSTICE ET AL., *supra* note 14, at 2.

Based on this, they can often extrapolate (or purchase from a data aggregator) an individual's age, gender, sexual orientation, race, career, income bracket, marital status, parenthood status, and much more.[48] They can also determine aggregate trends, such as buying patterns by time of year or demographic. Further, the company collects Social Security and driver's license numbers in a number of scenarios, such as when someone cashes a payroll check at a Walmart location.[49]

Users interact with Walmart in brick-and-mortar stores as well as through its website and mobile app. They consciously provide certain data points, such as their addresses and phone numbers when purchasing items online. In these cases, users physically input their data on the screen. In other instances, though, they may not be aware of the types of data the company can collect, such as customers' movements through a store, which can be tracked using cameras, GPS, Wi-Fi, or cellular triangulation.[50] Even if they are conscious of it, they may not have a choice—in many cases, Walmart is an easy and relatively inexpensive place to purchase necessities and access banking-like services.[51]

Walmart's data collection is an attempt to serve customers better, in one sense. The company wants to "optimize the shopping experience for customers when they are in a Walmart store, or browsing the Walmart website or browsing through mobile devices when they are in motion."[52] It is trying to anticipate the needs of its customers so that it can always have the right products stocked. It is also attempting to discover how best to push products that consumers might not otherwise buy. Using data mining techniques, Walmart can discover point-of-sale patterns in consumer behavior to provide

48. CJ Frogozo & Kayla Keller, *New Report: Walmart Gathering 'Big Data' That Can Be Used to Invade Privacy, Fuel Hidden Discrimination*, COLOR CHANGE (Nov. 27, 2013), https://colorofchange.org/press/2013/11/27/new-report-walmart-gathering-big-data-can-be-used-/ [https://perma.cc/65BN-WTPM].

49. Constance L. Hays, *What Wal-Mart Knows About Customers' Habits*, N.Y. TIMES (Nov. 14, 2004), http://www.nytimes.com/2004/11/14/business/yourmoney/what-walmart-knows-about-customers-habits.html [https://perma.cc/Z6LN-27GK].

50. *See* Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html [https://perma.cc/A4LS-L46E]; Stacey Gray, *In-Store Location Tracking: A Holiday Guide*, FUTURE PRIVACY F. (Dec. 22, 2015), https://fpf.org/2015/12/22/in-store-location-tracking-a-holiday-guid [https://perma.cc/BC7M-YBX7].

51. Deirdre Fernandes, *More Relying on Walmart for Financial Services*, BOS. GLOBE (July 10, 2014), https://www.bostonglobe.com/business/2014/07/09/walmart-isn-bank-but-consumers-are-choosing-its-financial-services/0oJtrqVKl8OXTuQ3SBtrSI/story.html [https://perma.cc/5T4U-3DJ2].

52. DEZYRE, *supra* note 46.

new product recommendations.[53] One better-known example was when it used data analytics to determine that before hurricanes, sales in strawberry pop-tarts increase by seven times their normal rate. As a result, stores began stocking them in larger amounts before hurricanes, which led to more people purchasing them.[54] As Walmart's CEO of Global Commerce said in 2013, "We want to know what every product in the world is. We want to know who every person in the world is. And we want to have the ability to connect them together in a transaction."[55]

2. Uber

Like Walmart, Uber has a wealth of sensitive information about its users. Users reasonably expect that Uber knows where they live and the locations they frequent; every time users interact with the app, they give the company data on at least two of their locations that day. The more often they use the service, the more Uber knows about their travel patterns. From this data, it is not hard to determine where someone works, lives, exercises, eats, and so on—any location that someone visits with regularity. Uber does not even require addresses; instead, a user may put in the name of a location (e.g., "Newark Airport" or "Starbucks"), allowing Uber to learn exactly *what* a user is visiting, rather than its location. This specificity provides Uber with information about not only users' travel patterns, but also their lifestyles—how many hours a day they spend at work, how often they sleep at home versus elsewhere, how frequently they visit a gym, what types of restaurants they go to, and much more.

Uber has a "strict policy prohibiting all employees at every level from accessing a rider or driver's data. The only exception to this policy is for a limited set of legitimate business purposes."[56] The policy does not define "legitimate business purpose" aside from examples of payment facilitation, solving problems for drivers or riders, monitoring accounts for fraudulent activity, and troubleshooting bugs. One can imagine a host of other "legitimate business purposes," including advertising or promoting the service, at the very least.

53. *Id.*

54. Hays, *supra* note 49.

55. DEZYRE, *supra* note 46; *see also* CTR. FOR MEDIA JUSTICE ET AL., *supra* note 14, at 17.

56. *Uber's Data Privacy Policy*, UBER (Nov. 18, 2014), https://newsroom.uber.com/ubers-data-privacy-policy [http://archive.is/TjxGV].

3. Facebook & Google

With Facebook and Google, we move into a different category, in which data sharing, collection, and usage is fundamental to the relationship between the company and the user. Not only do Facebook and Google collect data through their own websites, but they also provide data analytics tools to others. A recent study found that at least 77.4% of all websites track users' data; 60.2% of websites use Google trackers, and 27.1% use Facebook trackers.[57] This indicates that Google and Facebook also possess all of the data provided to these third-party sites as well.

People use Facebook to extend their existences onto the Internet—as "a medium for our personal lives"[58]—but they have an underlying expectation that the online experience should not change that personhood. But of course it does. Seeing pictures of friends at the beach may make them more likely to want to go to the beach, seeing a friend's book recommendation may inspire them to pick it up, reading about friends' reactions to President Trump may influence their feelings about the administration (or their feelings about their friends), and so on. Especially because Facebook's newsfeed shows them what their friends are doing, rather than showing strangers, the posts they see exert a higher level of influence. Similarly, if they are using Google to find out more about the world, they do not expect that it tailors its search results to their preferences or to promote its own agenda—they assume that the search results they see are roughly the same for everyone, and differences are based on some neutral categorization. But that is not always the case.[59]

Algorithms are only as good as the data put into them—if a data set is skewed, or if the code reflects its creator's implicit bias, the algorithm could be far from neutral.[60] An algorithm may treat every individual's data in the same way, but "software engineers construct the datasets mined by scoring systems; they define the parameters of data-mining analyses; they create the clusters, links, and decision trees applied; [and] they generate the predictive models

57. Many websites use multiple trackers from multiple third-party sources. *Tracking the Trackers*, GHOSTERY (Dec. 4, 2017), https://www.ghostery.com/lp/study [https://perma.cc/CH9L-WM3F]; *see also* Macbeth, *supra* note 6.

58. Lev Grossman, *Person of the Year 2010: Mark Zuckerberg*, Time (Dec. 15, 2010), http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183_2037185,00.html [https://perma.cc/QES3-59GD].

59. For a list of public updates to Google's algorithm, see *Google: Algorithm Updates*, SEARCH ENGINE LAND (last visited Nov. 20, 2017), http://searchengineland.com/library/google/google-algorithm-updates [https://perma.cc/A2V8-FYUH].

60. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 2 (2014) ("There is nothing unbiased about scoring systems.").

applied."[61] Even the simple choice to include or exclude a certain variable can skew an algorithm's results.[62] The assumption that algorithms are neutral is not just incorrect, but also potentially dangerous, as users may assume results are neutral.

It is well-documented that Facebook and Google use data to advertise, improve their newsfeed and search algorithms, and more.[63] The companies have the ability to know or extrapolate users' political leanings, eating and dating habits, credit and job histories, and more. Both have a massive amount of information about each of its users, including "your age, gender, location, and everything you search for."[64] All of this information is incredibly useful for advertising, but it can be utilized for a number of purposes, some of which would breach users' trust. And separately, users might expect their Google search or Facebook feed to be "neutral"—that is to say, a representative sample of what other users see—when, in fact, the service provider can tailor its results to each individual viewer, based on what it knows about the user. This is not *necessarily* a breach of the fiduciary duty, but as the next Part demonstrates, it might be.

---

61. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 35 (2015).

62. *See* danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC'Y 662, 667 (2012) (noting that the process of "making decisions about what attributes and variables will be counted[] and which will be ignored . . . is inherently subjective").

63. *See, e.g.*, Christine Erickson, *Google Privacy: 5 Things the Tech Giant Does with Your Data*, MASHABLE (Mar. 1, 2012), http://mashable.com/2012/03/01/google-privacy-data-policy/ [https://perma.cc/TJ2G-95UM]; Mark Hachman, *The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers*, PCWORLD (Oct. 1, 2015, 3:00 AM), http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html [https://perma.cc/DKW2-UNC2]; Victor Luckerson, *7 Controversial Ways Facebook Has Used Your Data*, TIME (Feb. 4, 2014), http://time.com/4695/7-controversial-ways-facebook-has-used-your-data [https://perma.cc/2AWF-CKP5]; Bernard Marr, *How Facebook Is Using Big Data: The Good, the Bad, and the Ugly*, LINKEDIN (July 16, 2014), https://www.linkedin.com/pulse/20140716060957-64875646-facebook-and-big-data-no-big-brother [https://perma.cc/GAA5-G286]; Steven Rosenfeld, *4 Ways Google Is Destroying Privacy and Collecting Your Data*, SALON (Feb. 5, 2014, 12:50 PM), www.salon.com/2014/02/05/4_ways_google_is_destroying_privacy_and_collecting_your_data_partner [https://perma.cc/4U62-LXHC].

64. *See* Jeff Parsons & Sophie Curtis, *How to See Everything Google Knows About You—and Switch It OFF*, MIRROR (Aug. 21, 2017, 11:51 PM), www.mirror.co.uk/tech/how-much-google-really-know-7685863 [https://perma.cc/YSK6-VXZF].

III. BREACHING FIDUCIARY STATUS: FOUR MAIN PRINCIPLES

This Part attempts to elucidate the information fiduciary duty by defining four categories of behavior: manipulation, discrimination, third-party sharing, and violating a company's own privacy policy.[65] These principles were developed by the author through an examination of dozens of real and hypothetical data usage scenarios, which gave rise to common themes that emerge when people oppose specific instances of data usage. According to each principle, some practices would be permissible for information fiduciaries, while others would not. This Article posits that what separates an acceptable practice from an unacceptable one is users' expectations: if a service provider is using data in a way that reasonable users would not expect, the service provider may have violated its duty. Writ large, the reasonable person—as defined by the author and informed through public reactions to various instances of data usage over the last decade—would not expect a service provider to manipulate her with her data, discriminate against her using information it has about her, or share her data with third parties without her consent.

Additionally, the fourth principle—that service providers adhere to their own privacy policies—illuminates a crucial point regarding consent. A reasonable user would not expect a service provider to use her data in a way it has promised it would not, and so it is part of the information fiduciary duty for that reason. But it also highlights something particularly important about the information fiduciary duty: a reasonable user's expectations can—and should—shift in response to various prompts. If a company notifies users of a particular practice, that practice should come within the users' expectations. Users could then choose, of their own accord, whether or not to use the service.[66]

But since it may not be possible—and certainly would not be easy—for most people to choose not to use services like Google going forward, user notification should not be a complete safe harbor. Manipulation and

65. Before diving deeper into the principles, however, it is worth noting that the fiduciary duty may not be owed to users alone; service providers may also owe a fiduciary duty to employees and independent contractors, who are also sources of data. And like users, employees and independent contractors have to simply trust that the service provider will not misuse their data. So although this Article discusses users, the protection should be extended to anyone who trusts a service provider with their personal data, such as the company's employees.

66. Although, as the author will argue, *see infra* Section III.D, privacy policies should be clearer and shorter if this is to work.

discrimination should always breach the duty, regardless of notification practices. And requiring information fiduciaries to behave in accordance with all four of these principles would also provide a level of standardization for data protection, which would "help products and services to meet consumers' expectations" because it is easier to align expectations with reality through standardization.[67]

If users reasonably trust a company with their data, the company is an information fiduciary and should act accordingly by respecting its users' trust and expectations. If a service provider fails to do so, it will have violated its fiduciary duty and should face legal consequences. When incorporated into the duty, these four principles will adequately protect users while still allowing service providers to innovate and profit. Ideally, the hypotheticals posed after the explanation of each principle will help readers visualize the lines that must not be crossed: what would a fiduciary duty look like for service providers in practice, and how would it change the status quo? This Article focuses mainly on a set of four companies to provide consistency, but also to show how the duty varies for service providers as diverse as big box stores, ride-sharing apps, and websites that simultaneously provide social media, news, communication tools, and much more.

A. ANTI-MANIPULATION OF THE USER

A first principle of the fiduciary duty revolves around manipulation: when a company uses information about users to surreptitiously manipulate them, it may breach its fiduciary duty. And often, the user has no easy way of knowing whether and how it is happening. Cass Sunstein defines a manipulative statement or action as one that "does not sufficiently engage or appeal to people's capacity for reflective and deliberative choice."[68] Defined as such, manipulation can manifest in two ways: (1) a failure to respect people's autonomy and an affront to their dignity; or (2) promotion of the welfare of the service provider over that of the user.[69] Importantly, an action is not manipulative simply because it is an attempt to alter another person's behavior; "manipulation" is different from providing facts or attempting to persuade through reason. Instead, manipulation requires an attempt to circumvent the other person's "capacity for reflection and deliberation."[70] In other words,

67. *See How Standards Benefit Consumers*, ISO, http://www.iso.org/sites/ConsumersStandards/2_benefits.html (last visited Feb. 28, 2018) [https://perma.cc/ZC8D-NB6L].

68. Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MARKETING BEHAV. 213, 239 (2015).

69. *Id.* at 217–18.

70. *Id.* at 216.

covertness is the real concern, because users are not able to engage with the service provider or recognize its motives.

This Article draws on Sunstein's definition and analysis of manipulation to explore how service providers might manipulate users in a way that violates their fiduciary duty. As I will demonstrate, much of this would be outside what a user would reasonably expect—or detect—and thus would violate most users' trust.[71]

1. A Dignity- and Autonomy-Focused Conception of Manipulation

In one respect, manipulation is a problem because it can "violate people's autonomy (by making them instruments of another's will) and offend their dignity (by failing to treat them with respect)."[72] In other words, manipulation is problematic when it leads someone to make a choice on terms other than their own, "depriv[ing] people of agency" or humiliating them.[73] Manipulation in this way breaches the trust that users place in a company when they hand over their data. Users do not expect that companies will an attempt to alter their choices or decisions by using their data, particularly when the company's decision to do so is driven by its own agenda. While Google uses data to determine which websites to display in search results, the expectation is that this is an attempt to improve the service by showing the most relevant results—not an attempt to get people to do something that they would not have done otherwise. Surreptitiously manipulating the user on an important issue, such as an election, takes away users' autonomy and disrespects their conception of "self." The fiduciary duty—designed to diminish information asymmetries—can leave no room for service providers to implement this kind of covert action.

2. A Welfarist Conception of Manipulation

In another respect, the problem with manipulation stems from the prioritization of one party's welfare over the other. As Sunstein explains:

71. Of course, service providers will not and should not treat all users the same; in many ways, customization is one of the advantages of the information age, for users and businesses alike. But as Jonathan Zittrain puts it, "[m]y search results and newsfeed might still end up different from yours based on our political leanings, but only because the algorithm is trying to give me what I want—the way that an investment adviser may recommend stocks to the reckless and bonds to the sedate—and never because the search engine or social network is trying to covertly pick election winners." Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/AY8J-J7C2].

72. Sunstein, *supra* note 68, at 217.

73. *Id.* at 226.

"People know what is in their best interests and should have a (manipulation-free) opportunity to make that decision."[74] Service providers engaging in this kind of manipulation may utilize data to maximize their own welfare while sacrificing the welfare of users. Users are thus deprived of the "ability to make choices on their own, simply because they are not give[n] a fair or adequate chance to weigh all variables."[75] Service providers may not have a full and accurate picture of users' "situation, tastes, and values," but they "nonetheless subvert[] the process by which choosers make their own decisions about what is best for them."[76] And if the service provider is maximizing its own self-interest, it would violate the archetypal fiduciary duty: the "special obligations of loyalty and trustworthiness toward another person. . . . The [user] puts . . . trust or confidence in the fiduciary, and the fiduciary has a duty not to betray that trust or confidence."[77] But because users typically are unable to understand or monitor how service providers use their data, a fiduciary duty must require companies to prioritize their users' interests over their own.[78]

3. Targeted Advertising

The anti-manipulation principle runs up against the idea that targeted advertising—or, indeed, any advertising—is manipulative. Of course this is the case: the advertisements users are shown are meant to manipulate them into buying the featured items. Advertising is directed toward changing behavior; if someone leaves an item in a virtual shopping cart without purchasing it, an advertisement reminds her to go through with the purchase. When an advertiser shows a user a brand of makeup that is similar to the one she typically buys, it is trying to convince her to switch brands. But, crucially, users are conditioned for this; they are familiar with the concept of advertising and know that ads are meant to manipulate them. They expect service-providers will display advertisements meant to change their behavior. When they see an ad, they meet it on "equal footing"[79] and can consciously decide whether to change their behavior based on that ad. As Sunstein puts it:

> In an advertising campaign, everyone knows the nature of the interaction. In some ways, manipulation is the coin of the realm. The purpose of advertisements is to sell products, and while we can find purely factual presentations, many advertisements do not appeal to

74. *Id.* at 213.
75. *Id.* at 228.
76. *Id.*
77. Balkin, *supra* note 21, at 1207.
78. *See id.* at 1227.
79. *Id.* at 1216.

> reflection or deliberation at all. They try to create certain moods and associations. *To the extent that the enterprise is broadly understood, and to the extent that users understand it, the ethical objections are weakened; people can and do discount self-interested efforts at manipulation.*[80]

And because of this, it is rare that the platform providing the advertising—whether print or online—is viewed as a trusted advisor in that realm. For example, there is no evidence to suggest that people trust Facebook as an advisor on the variety of products advertised through its platform, such as dating services, mortgage lenders, clothing stores, and more. Targeted advertising can be consistent with a service provider's fiduciary duty because the manipulation is not covert. Advertising is an understood component of the relationship between a service provider and a user; it does not defeat the expectations of the end-user, even when a service provider manipulates their algorithm to better target an individual based on the data the company has about that person.

In that sense, targeted advertising is fundamentally different from a company manipulating users in a way that defeats their expectations by covertly pushing an agenda or promoting its own welfare at its users' expense. In the first case, the agenda-pushing defeats expectations because it deprives users of agency in decision-making. In the second case, users resent the welfare-maximizing behavior as an abuse of the position of power enjoyed by the service provider. And so both forms of manipulation are unlike targeted advertising in that users neither presume that the behavior is happening nor have the information necessary to engage with the company in an informed manner. That is to say, users are familiar with the concept of advertising and usually understand that an advertisement is meant to manipulate; users are less trained to expect (and detect) manipulation from service providers and data collectors. As a result, they cannot engage with service provider manipulation in a meaningful way.

4. Hypotheticals[81]

a) Walmart Pushes an Anti-Abortion Agenda

Assume Walmart's management and Board of Directors is staunchly anti-abortion. They make sure their website always displays sale prices for books about the mental and physical dangers of abortion, and they direct their web engineers to ensure that when someone searches online for forms of birth

80. Sunstein, *supra* note 68, at 227 (emphasis added).

81. Except where noted or cited, the hypotheticals throughout this Article are fabricated or designed to make a particular point. The author does not put forth any allegations outside of those that have been publicly reported. Any hypotheticals based on public reports have footnotes indicating the sources.

control, the results display those same books as well as advertisements featuring adorable babies. This strategy seems manipulative, but it would not violate Walmart's fiduciary duty. The key is that the company is not using each individual's data to manipulate them. Assuming these results are the same for all users, the company is free to push an agenda on customers out in the open.

But change the hypothetical so that Walmart only implements this practice for users whom it believes are white, in an effort to dissuade only white women from terminating pregnancies. This practice would violate the company's fiduciary duty. Walmart is now using a piece of data it has about the user to change its typical search results and push an agenda surreptitiously, convincing white women to have babies while letting women of other races search for birth control unimpeded. This strategy diminishes the users' autonomy in making decisions about their own health. Additionally, not only would Walmart be violating the anti-manipulation principle by using individual users' data to push an agenda, it would also violate the discrimination principle by manipulating certain groups of people based on their race and gender.[82]

b) Uber Performs Psychological Experiments on its Drivers

In April 2017, it was revealed that Uber had performed "psychological tricks" on its employees,[83] to whom, as noted earlier, service providers should also owe a fiduciary duty.[84] In order to make up for its inability to require drivers to work at certain times, Uber "experimented with video game techniques, graphics and noncash rewards of little value that can prod drivers into working longer and harder—and sometimes at hours and locations that are less lucrative for them."[85] Uber used to have local managers text drivers "all day long, every day" about when the morning rush had started and where demand was highest.[86] While potentially annoying, this practice is acceptable—drivers know what is happening and why, and they can engage and respond with full knowledge.

But in addition, certain male local managers adopted female personas because most drivers are male—the theory was that men would be more likely to work harder and longer when women were the ones encouraging them to

82. The next Section describes the antidiscrimination principle in more detail.

83. Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers' Buttons*, N.Y. Times (Apr. 2, 2017), https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html [https://perma.cc/W8ZD-U9HA].

84. *See supra* note 65.

85. Scheiber, *supra* note 83.

86. *Id.*

do so.[87] Uber also began using tricks well known by psychologists and video game designers: by covertly getting drivers to "internalize the company's goals,"[88] drivers became more motivated to work longer hours. For example, research showed that drivers who completed twenty-five rides were more likely to continue driving, so Uber began sending messages at certain points, such as, "You're almost halfway there, congratulations!"[89] When drivers attempted to log out for the day, the app would "tell them they were only a certain amount away from making a seemingly arbitrary sum for the day, or from matching their earnings from that point one week earlier."[90] The messages were based on another psychological finding regarding people's preoccupation with achieving goals. The company also introduced "badges" for goal achievement, another tactic cribbed from the video game industry.

Each of these tactics should be analyzed separately to determine whether a fiduciary duty would have been breached. The badges, for example, might be acceptable—a reasonable user/driver would know that these badges are meant as encouragement for driving more and can decide to use them as motivation or to ignore them. But the use of a female persona to encourage drivers to work more is less predictable and, thus, more covertly manipulative in two ways: it removes a driver's autonomy by forcing him to make decisions based on false information, and it enhances Uber's welfare possibly at the expense of its drivers.

To be sure, as an Uber spokesperson maintained, nothing stops drivers from ending their days; they are in literal control of that decision.[91] But surreptitious tricks could be unfairly manipulative by "depriv[ing] [drivers] of agency" because they are not making decisions on their own terms.[92] Put another way, drivers' ultimate decisions may incorporate Uber's influence without them realizing it, even as Uber presents itself as a company where drivers have more agency and flexibility.[93] Nudges may be expected in areas like targeted advertising to users, but application of these "psychological

87. *Id.*
88. *Id.* (quoting Chelsea Howe, a video game designer).
89. *Id.*
90. *Id.*
91. *Id.*
92. Sunstein, *supra* note 68, at 226.
93. *Driving Jobs vs Driving with Uber*, UBER, https://www.uber.com/driver-jobs [http://archive.is/bKXlX] (last visited Feb. 28, 2018) ("The best part about driving with Uber is that you can set your own hours. On the other hand, driving jobs, like driving a bus, can have very long hours and strict schedules. The opportunity that works best for you depends on whether you want a traditional full-time or part-time job, or want to work whenever you choose.").

levers"[94] to the workforce could violate the trust of employees. Drivers are not aware of the manipulation, and Uber is "using what [it knows] about drivers, their control over the interface, and the terms of transaction to channel the behavior of the driver in the direction they want it to go."[95]

c) Facebook Pushes a Political Agenda, Part I

Jonathan Zittrain has posed a hypothetical about "digital gerrymandering": on election day, Facebook "nudges" a subset of users to vote by showing them "a graphic containing a link for looking up polling places, a button to click to announce that you had voted, and the profile photos of up to six Facebook friends who had indicated they'd already done the same"—but the subset includes only those who are sympathetic to Mark Zuckerberg's preferred electoral candidate.[96] And as Zittrain argues, "the people with the most cause for complaint are those who won't be fed the prompt and may never know it existed."[97]

This practice violates the fiduciary duty by manipulating users to act in certain ways regarding important issues like elections. The service provider would be utilizing users' data to pinpoint their political preferences and push them toward a particular action (or inaction). This violates users' trust; people use Facebook on the assumption that the companies will not try to manipulate them to vote (or not vote) based on the sensitive information collected about them. Although the act of showing certain users links to find polling places is not itself manipulative, doing this on a large scale and differentiating between users based on their preferences is manipulative. Users know that Facebook's algorithm responds to their political preferences—a user tagged by Facebook as "liberal" might see articles about Senator Elizabeth Warren and global warming rallies more than a "conservative" user. And generally, users prefer this; many users like that the algorithm makes Facebook's newsfeeds more individually relevant. However, the expectation is that the algorithm changes *in the same way* for every user—liberals see liberal posts and conservatives see

94. Scheiber, *supra* note 83.

95. *Id.* (quoting Ryan Calo, a law professor at the University of Washington); *see also* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623, 1630–31 (2017).

96. Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/75BU-DF3N].

97. *Id.*

conservative posts.[98] That is not the same as manipulating the algorithm so that liberal users have *more* relevant or helpful posts than conservatives do. The latter manipulation violates the trust of users, who would not reasonably expect Facebook to attempt to change their behavior in this way.

d) Google Partners with Payday Lenders for Advertising

Payday lenders in the United States often use manipulative and exploitative tactics, setting the most vulnerable consumers up to fail.[99] They advertise on the Internet, including on Google, but that does not make Google liable for their practices. But might Google's partnerships with payday lenders go further than a typical targeted advertising relationship? Companies in the financial services industry are a lucrative source of income for Google. "[T]he three most expensive categories of keyword searches as measured by cost per click are in financial services (insurance, loans and mortgages), with 45.6 percent of the top 10,000 advertising keywords falling in those categories."[100] Google's practice of soliciting advertisements from payday lenders is acceptable, but one reporter found that "Google is burying bad news about the industry for consumers."[101] He discovered that Google "placed the uniformly negative news items [about payday lending] near the bottom of the results, below the fold as we used to say in the newspaper business."[102] If this is in fact the case, Google is in breach of a theoretical fiduciary duty because it is manipulating users to enhance its own welfare at the users' expense. This kind of manipulation is unexpected by users; while Google's search results often change based on the user, a reasonable user would not expect that the algorithm *hides information* based on who spends the most to advertise with Google.[103]

98. This may not be beneficial, writ large, but the debate on political and media silos is outside the scope of this Article.

99. Press Release, Consumer Fin. Prot. Bureau, Consumer Financial Protection Bureau Proposes Rule to End Payday Debt Traps (June 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-proposes-rule-end-payday-debt-traps [https://perma.cc/EK9X-KXMG].

100. Nathan Newman, *Why Google's Spying on User Data Is Worse than the NSA's*, HUFFINGTON POST (July 1, 2013, 4:06 PM), www.huffingtonpost.com/nathan-newman/why-googles-spying-on-use_b_3530296.html [https://perma.cc/F9WL-5E2J].

101. *Id.*

102. *Id.*

103. And while it is true that the consumer-focused websites were shown, research has demonstrated that Google's interface gives users the "impression that the search results imply a kind of totality," but "one only sees a small part of what one could see if one also integrates other research tools." *See* H. MAURER ET AL., REPORT ON DANGERS AND OPPORTUNITIES POSED BY LARGE SEARCH ENGINES, PARTICULARLY GOOGLE 16 (2007),

Some have accused Google of maintaining "ads from fraudulent mortgage 'loan modification' firms preying on desperate homeowners even after the company was alerted to the problem."[104] This is likely not a form of manipulation unless Google's Terms of Service promise that it will not show advertisements from these kinds of companies. Google should not be held liable for displaying advertisements from companies that implement illegal practices. Not only would it be overly burdensome for Google to have to look into its advertisers' practices—in a wide variety of industries, all with different regulations—but it should also be unnecessary for a fiduciary. Because this falls into the category of targeted advertising, we should trust users to know an advertisement when they see it. Google should not be on the hook for every bad actor who buys advertisement space.

B. ANTIDISCRIMINATION

The second principle that information fiduciaries must follow is antidiscrimination, or refraining from discriminating between or against users based on characteristics like race or gender. The set of data points available to companies often includes these qualities and many others. There are three main methods by which a company might discriminate based on these characteristics: (1) access to services, (2) prices, and (3) digital redlining. As a fiduciary, a firm must not offer different services or prices to individuals based on their membership (or non-membership) in a protected class. Users likely do not expect that when they hand over their data online, they are making it easier for companies to discriminate against them or others, or that the company will in fact do so. If users do not expect this type of practice, they cannot reasonably guard against it by choosing service providers more carefully or choosing not to provide certain data about themselves. Companies can triangulate to figure out a user's characteristics (for example, extrapolating someone's age and gender from the websites they visit and products they buy), and users are unlikely to expect or believe that they should hide this information about themselves.

Furthermore, users often have no choice but to provide their data—not just because it is difficult to operate in the modern world without Google or Facebook, but also because many other important services require it. For example, to cash a payroll check at Walmart—a service relied on by many

http://www.iicm.edu:8080/Ressourcen/Papers/dangers_google.pdf [https://perma.cc/ZF4G-GZUR].

104. Newman, *supra* note 100.

people with low income[105]—you must give them your Social Security number, which opens the door to a host of data about the customer.[106] Because service providers have an immense upper hand in gathering and using this information, they should be required to treat it with the utmost care.

When considering "discrimination," it is important to determine what qualities service providers could use to discriminate. Many are those that define membership in a protected class: race, color, religion, national origin, age, sex (gender), sexual orientation, and physical or mental disability.[107] However, Big Data makes it unwise to focus only on traditional targets of discrimination, such as racial minorities. As more data emerges, it may become the case that the people against whom firms discriminate do not correspond with the traditional categories listed above. When service providers collect data that lets them identify and categorize users by hundreds of categories, it becomes easier to isolate and discriminate against a new group: those who are less "valuable." For example, it may be the case that white men of a certain socioeconomic status and in a certain geographic area are less valuable to service providers because fewer advertisers are interested in reaching them. And, as with all discrimination, offering certain services or products only to "valuable" groups further entrenches divisions or silos that already exist. The antidiscrimination principle, then, involves a moving target that will need to be reassessed periodically to identify who may be harmed or left behind by algorithmic decision-making.

1. Access to Services

One way in which companies could discriminate against users is by offering different services to different people. For example, if a Facebook algorithm determines that the data of young people is more valuable than the data of older people, it could continue offering Facebook for free to young people, while providing older people with only a pared-down, barer platform. Or, the company could provide more tools or apps for younger people than older people. A company might not want to waste expensive server space on users who generate less advertising revenue. More subtly, this type of discrimination could be mixed in with a "freemium" model of services, which

105. About a fifth of Walmart customers are unbanked, and Walmart processes 1.2–1.4 million money orders, wire transfers, and cashed checks per week. JEAN ANN FOX & PATRICK WOODALL, CONSUMER FED'N AM., CASHED OUT: CONSUMERS PAY STEEP PREMIUM TO "BANK" AT CHECK CASHING OUTLETS 14 (2006), http://www.georgiawatch.org/documents/CFA2006CheckCashingStudy_000.pdf [https://perma.cc/JB9M-PDZT].

106. Hays, *supra* note 49.

107. *EEO Terminology*, NAT'L ARCHIVES (Aug. 16, 2015), https://www.archives.gov/eeo/terminology.html#d [https://perma.cc/ZT3L-4NJE].

typically offers a basic service for free and then charges a price for the premium service. For example, Spotify offers its basic platform for free, but charges a monthly fee for users to avoid commercials and access the platform on more than one device.[108] Spotify could easily alter this model to create different options for different users based on certain characteristics, such as age, gender, profession, geolocation, amount of money spent with other service providers, and much more.

Service discrimination likely defies most users' expectations of service providers when they engage in a typical online transaction. When people use Facebook, they do not expect that they are seeing more or fewer features (for example, a newsfeed, group invitations, or applications like Candy Crush) based on their personal characteristics. Imagine if Facebook only offered newsfeeds or posting capabilities to people who make a certain amount of money or work in certain fields—this kind of discrimination would undermine the expectations of all users. When those users provided Facebook with their information, it likely never occurred to them that the information could then be used to limit or grant access to specific features. A service provider would be breaching its fiduciary duty by using the data users provided to offer them an incomplete suite of services.

To be fair, tailored services are often seen as a feature of Big Data, rather than a bug. The fact that a service provider can change services based on a user's interests can improve the service itself: for example, if Facebook knows that a user is a runner, and thus proactively offers a free running map application to that user, it may be mutually beneficial for both user and service provider. And someone who prefers Game of Thrones fan fiction to running may prefer that Facebook populates her newsfeed with Game of Thrones fan pages instead of a running map application. But this is not discrimination as long as the services are *available* to both people. A service provider can affirmatively offer services to users who might be interested, but to be a fiduciary, it should not *prevent* any user from accessing a service that is available to some. The runner may have to actively search for the Game of Thrones pages if she wants to view them, but as long as they are available to her, the practice is consistent with the fiduciary duty.

108. Pascal-Emmanuel Gobry, *How Spotify's Business Works*, BUS. INSIDER (Oct. 12, 2011, 12:53 PM), http://www.businessinsider.com/how-spotifys-business-works-2011-10 [http://archive.is/yYtct].

2. Price Discrimination

Data collection also makes price discrimination easy. A company could identify who might be more likely to pay higher prices or at what times they are more likely to do so and then shift pricing based on that information. For example, Walmart could increase the price for pop-tarts before a hurricane, as noted above,[109] or Uber could charge women more at night based on data that women are more likely to take cars than they are to walk after dark. Both of these practices might be based on data and algorithmic results. The first example would be permitted because it does not target a specific group of people. The change in pop-tart pricing would be based on publicly available data, such as timing and weather patterns. But the second example should be prohibited for fiduciaries, since it disadvantages a group based on data about users' gender obtained for another purpose.

Of course, price discrimination occurs all the time, such as with senior citizen discounts or variance in gas prices.[110] But these are instances of price discrimination about which users are aware. Senior citizen discounts are clearly posted, and a reasonable driver knows that gas prices vary by location, mirroring the other cost-of-living adjustments she sees in different parts of the country.[111] More often than not, comfort with certain types of price discrimination coincides with user expectations having been shifted. A user of an online service provider, however, cannot tell if "companies are offering discounts to higher-status customers in the first place."[112] Few would expect that the prices for items like kitchen tools or clothing on a standard website change based on who is viewing the item. And it would be quite difficult to identify when a company adds a dollar to certain products if it believes the person viewing them online is black, for example, especially because false negatives and positives would occur and confuse even rigorous analyses.[113]

109. As discussed earlier, Walmart's data shows that strawberry pop-tart sales increase seven-fold before hurricanes. Hays, *supra* note 49.

110. *See* Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), http://www.wsj.com/news/articles/SB10001424127887323777204578189391813881534 [https://perma.cc/LC2P-3WWW].

111. *See Gasoline and Diesel Fuel Update*, U.S. ENERGY INFO. ADMIN. (Nov. 23, 2017), https://www.eia.gov/petroleum/gasdiesel/gas_geographies.php#pricesbyregion [https://perma.cc/Y96J-HQGW].

112. Jeffrey Rosen, *Who Do Online Advertisers Think You Are?*, N.Y. TIMES (Nov. 30, 2012), http://www.nytimes.com/2012/12/02/magazine/who-do-online-advertisers-think-you-are.html [https://perma.cc/KZM8-CGFG].

113. This is not a worst-case scenario supposition either. As a 2013 article notes, people of color and low-income communities face particular risks. The "poverty exception" to privacy rights has been explored previously, *see* Christopher Slobogin, *The Poverty Exception to the Fourth*

This type of conduct undermines the economic and psychological interests of users by utilizing their data to discriminate more efficiently.

There is no way for a single user to know whether they are seeing a higher price online than someone of a different race sees and no cost-effective way for them to figure it out. And fiduciaries should not engage in practices that force consumers to band together to police them. Because this type of discrimination is both economically harmful and opaque, it is unreasonable to expect users to know whether a company is using information it has about them to decide what to charge them for goods and services. Users cannot engage with the service provider on an equal footing in this context, and the company is abusing its power and breaching users' trust.

3. Digital Redlining

While it is not clear that many companies are currently offering different services or prices based on membership in a protected class, service providers can discriminate by zip code, which can often be a proxy for membership in a protected class. Though now illegal, practices such as redlining[114] have enabled this type of discrimination in the past. Now, this type of discrimination is easier with Big Data. Internet Protocol (IP) addresses can be linked to zip codes—this allows most firms to know where their users are when they access a website.[115] There is no general statute that proscribes online service companies from shifting their service offerings or prices by zip code. And even if they are using zip codes in this way, it may be defensible in court as a business necessity—assuming a user could even figure out that the practice is occurring and get into court.

Amendment, 55 FLA. L. REV. 391, 412 (2003), and the risks of bias or discrimination based on the inappropriate generation of personal data—what have been called "predictive privacy harms"—are well-documented, *see* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 95 (2014); *see also* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25 (2013); Kevin Tobia, Note, *Disparate Statistics*, 126 YALE L.J. 2382 (2017).

114. Redlining is "the illegal practice of refusing to offer credit or insurance in a particular community on a discriminatory basis (as because of the race or ethnicity of its residents)." *Redlining*, MERRIAM–WEBSTER, https://www.merriam-webster.com/legal/redlining [http://perma.cc/6BFU-6469].

115. *See, e.g.*, *Geolocate IP Address Location Using IP2Location*, IP2LOCATION, https://www.ip2location.com [https://perma.cc/FU34-K2DN] (last visited Feb. 28, 2018); *IP Address Lookup*, WHATISMYIP.COM, https://www.whatismyip.com/ip-address-lookup [https://perma.cc/DP4X-36A2] (last visited Feb. 28, 2018).

Of course, markets and demand differ across the United States; it is understandable that Uber might charge more in an established market like New York than in a market in which it is newer and less popular. It is not only understandable, but perhaps preferable, that when one searches for restaurants on Google, the search results show places in the user's area.[116] Information fiduciaries exist in a vast number of industries, some of which appropriately discriminate by zip code. For example, nanny services offered via Care.com are more expensive in San Francisco, California than they are in areas with lower costs of living, like Fargo, North Dakota.[117] The ability to adjust pricing according to cost of living is not in itself problematic.

But price differentials should be tied to market demand rather than racial or other biases. To use mortgage lending as an analogy: houses are priced based on their location, but they cannot be priced differently based on the buyer's identity. In the former case, the price is derived from market demand; in the second, it could be derived from discrimination. A similar principle should apply across the board—demand differs by market, and prices can adjust accordingly. But prices should not differ based on buyers' identities. If a geolocation-based practice were challenged in court, a "substance-over-form"-like doctrine[118] should be applied; a court could consider whether, agnostic of any protected class disparities, market economics demanded differential pricing or services in specific areas.

In certain cases, geographic discrimination might be consistent with a fiduciary duty. Discover has "show[n] a prominent offer for [its] new 'it' card" to users in particular cities and Rosetta Stone has offered discounts and

116. However, this justification can become a slippery slope: proponents of redlining in the mortgage space also argued that it simply made sense from a business perspective to refuse to lend in certain areas. But this practice "perpetuate[s] historical conditions . . . [and] helps to promote a racially separate and unequal distribution of political influence and economic resources." Richard Thompson Ford, *The Boundaries of Race: Political Geography in Legal Analysis*, 107 HARV. L. REV. 1841, 1844 (1994).

117. *Compare San Francisco Nannies*, CARE.COM, https://www.care.com/nannies/san-francisco-ca [https://perma.cc/77UC-3GYC] (last visited Feb. 28, 2018) (listing the average price for a nanny in San Francisco as $17.25 per hour), *with Fargo Nannies*, CARE.COM, https://www.care.com/nannies/fargo-nd [https://perma.cc/W923-R6DV] (last visited Feb. 28, 2018) (listing the average price for a nanny in Fargo as $10.75 per hour).

118. In tax, the substance-over-form doctrine allows a court to "recharacterize a transaction in accordance with its substance, if 'the substance of the transaction is demonstrably contrary to the form.' " DEP'T OF TREASURY, THE PROBLEM OF CORPORATE TAX SHELTERS DISCUSSION, ANALYSIS AND LEGISLATIVE PROPOSALS vii–viii, 47 (1999). In other words, if the court can tell a litigant was trying to achieve one outcome while making it look like something else, the court can respond to the reality of the transaction, not its appearance. *See id.*

"bundles" in particular locations.[119] These are plausible cases in which a non-discriminatory market analysis might explain the company's decision. On the other hand, ProPublica discovered that "Asians were nearly twice as likely to get [a] higher price from The Princeton Review than non-Asians" for an SAT course.[120] Prices were charged based on zip code, not based on race, but in at least one example, a Queens zip code with 70.5% Asian residents but a below-median average income was charged the highest price possible for the course.[121] Absent another justification for the pricing disparity, it seems that Princeton Review may have specifically targeted Asians, as the disparity cannot be explained only by the zip code's average income level.[122] Even if one argues that Asians *are* more likely to pay higher prices for SAT courses, and so Princeton Review was simply responding to market demand, service providers should not be permitted to use the data they have on users' race to respond to market demand. Users who provided that information when signing up for a course online would never have expected that data to be used to then charge them a higher price.

4. Hypotheticals

a) Advertising Products Based on Broad Demographic Preferences

Many retailers' websites show products that a user might like based on other items the user has purchased or browsed. Assume a person buys L'Oréal shampoo from Walmart every few months, and assume Walmart's data demonstrates that when L'Oréal's price goes up, women typically switch to Dove shampoo, while men switch to Suave. Walmart might share this finding with Dove and Suave, who could then pay Walmart to show advertisements for Dove to women and Suave to men who search for L'Oréal online. This practice would be entirely consistent with the fiduciary duty. Even though the

119. Valentino-DeVries et al., *supra* note 110.

120. Julia Angwin, Terry Parris Jr. & Surya Mattu, *When Algorithms Decide What You Pay*, PROPUBLICA (Oct. 5, 2016), https://www.propublica.org/article/breaking-the-black-box-when-algorithms-decide-what-you-pay [https://perma.cc/L3UY-7Z83].

121. Julia Angwin & Jeff Larson, *The Tiger Mom Tax: Asians Are Nearly Twice as Likely To Get a Higher Price from Princeton Review*, PROPUBLICA (Sept. 1, 2015, 10:00 AM), https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review [https://perma.cc/FT32-MGGT].

122. Certainly, there could be a third variable that explains the disparity, or the Rosetta Stone and Discover examples could be driven by a discriminatory motive. But absent additional information, the contrast between the two demonstrates that location-based "deals" can work if they do not discriminate based on sensitive user data.

advertising does "discriminate" based on gender, the discrimination is part of a targeted advertising campaign and is thus within users' expectations.[123]

However, assume Walmart instead determined that black people prefer L'Oréal and white people prefer Suave. Then, it chose to limit choices in a store in a predominantly black neighborhood and hike up the price for L'Oréal, and do the same for Suave in a predominantly white neighborhood. This would be an unacceptable use of race data. No longer is Walmart using data to perform targeted advertising with which users can engage on equal footing. Instead, in this second hypothetical, Walmart has skipped the advertising altogether and would be using data to charge higher prices for a product it knows that a certain demographic group wants.

b) Walmart Changes Shipping Prices Based on Zip Code

Walmart—and most stores—charge a shipping fee for online orders. Walmart may know that in high-income suburban neighborhoods where people are more likely to have cars, the user may just drive to the nearest store if the shipping fee is too high. The brick-and-mortar store they choose may or may not be a Walmart. In low-income neighborhoods where people may not have cars or easily accessible brick-and-mortar stores, users may be more likely to purchase certain items online, subjecting them to a shipping fee. Walmart could charge more for shipping in neighborhoods without easily accessible brick-and-mortar stores. This seems to violate the discrimination principle, though we may have to dig deeper.

It might be the case that it actually is more expensive to ship to these areas, though this is a more plausible argument for a zip code in a rural area than for a low-income zip code in a big city. And if Walmart could prove that the price hike was only given to those in neighborhoods where shipping is actually more expensive, it might survive a legal challenge. However, if Walmart were uniformly charging more in neighborhoods where no brick-and-mortar stores are nearby, regardless of the actual cost of shipping, it would be violating its fiduciary duty because users are not given a choice or enough information to make an informed decision. In the first shampoo example, users understand that they are being advertised to; here, there is no equivalent framework with which users are familiar.

123. On the other hand, the example in Section III.B.4.e below is not a targeted advertisement—it simply uses gender and other data to charge women more. No advertisement or notice is given.

c) Amazon Prime's Free Same-Day Delivery Service

Contrast Amazon Prime's Free Same-Day Delivery service, which, as of April 2016, was offered in twenty-seven metropolitan areas.[124] In many of those cities, "predominantly black ZIP codes" are excluded from the service.[125] In at least four cities, "black citizens are about half as likely to live in neighborhoods with access to Amazon same-day delivery as white residents."[126] Amazon maintains that zip codes are included or excluded based on the number of Prime members in those zip codes, and that it would be too expensive to include zip codes with few customers. It is at least plausible that this is true. But in Washington, D.C., the excluded zip codes east of the Anacostia River are quite close to downtown—closer, in fact, than some other D.C. metro areas that do receive same-day delivery service.[127] According to Google Maps, a zip code in Manassas, VA (20110) is 31 miles from the White House, the center of downtown D.C., and a zip code in Anacostia (20032) is 8.5 miles from the White House. But only the Manassas zip code receives the free same-day delivery service. If this were challenged in court, the court would need to delve deeper into the economics to decide whether this model violates the company's fiduciary duty. If exclusion of the black zip codes is, in fact, based on the fact that delivery to Manassas is significantly less costly than delivery to Anacostia, it might be acceptable. But if the economics do not quite make sense, the practice might violate the fiduciary duty.

d) Uber's Surge Pricing

Uber uses "surge pricing": when Uber is in high demand in a certain area, such as after a sporting event or during a rainstorm, prices are raised to ensure that those who are most willing to pay receive cars. This is basic market economics, and since everyone in the same area is offered the surge price at the same time, it is consistent with a fiduciary duty. But one can imagine a surge pricing-like technique that is similarly based on demand, but applied in a more discriminatory way. Imagine that Uber started charging women higher

124. Amit Chowdhry, *Amazon Adds 11 More Cities to Same-Day Delivery Service*, FORBES (Apr. 8, 2016, 3:19 PM), https://www.forbes.com/sites/amitchowdhry/2016/04/08/amazon-adds-11-more-cities-to-same-day-delivery-service/ [https://perma.cc/6Q5B-DAHF].

125. David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERG (Apr. 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day [https://perma.cc/8SJ2-EP3S].

126. *Id.*

127. Rachel Sadon, *Amazon Adds Free Same-Day Prime Delivery to D.C.—Well, Certain Parts of D.C.*, DCIST (May 29, 2015, 4:14 PM), http://dcist.com/2015/05/amazon_adds_free_same-day_delivery.php [https://perma.cc/WA9A-Z2Z7].

rates in cities at night because Uber's data demonstrates that women are more likely to pay a higher price for the service because they feel less safe walking home than a man would feel. Uber could implement this system by identifying every user's gender and shifting prices based on that information, the time of day, and the user's location. This is an example of data confirming, and possibly entrenching, stereotypes that already exist—the fact that data may seem to support a stereotype about a particular group of people should not be enough to permit a firm to take advantage of that stereotype.

This practice would violate the discrimination principle. Uber is choosing a class of people based on data it has about their gender—and a particular vulnerability due to that gender—and charging them more. When users entrust Uber with their data, they should reasonably expect surge pricing, because the app makes it clear when it is happening through an alert. However, users have no reason to expect or predict that Uber will also exact a "vulnerability fee" because it knows when a user is a woman. By doing so, Uber would violate users' trust.

e) Facebook Buys a Mortgage Lender

Facebook could purchase a mortgage lender and make it a subsidiary of its holding company. It could then potentially allow loan officers at the subsidiary to access users' Facebook data or social networks when deciding whether or not to extend credit to those users.[128] Certainly, discrimination based on race, gender, national origin, or something similar would be illegal under existing law. But assume the loan officers do not incorporate any of that data into their decisions. Instead, they focus on other things about you—your spelling and grammar, your educational background, your friends, your social activities, and more. A lender cannot refuse to extend credit based on an applicant's race, but can she refuse to lend (or raise the price) based on the race or education level of a prospective borrower's friends?[129] What about the fact a user frequently misspells words in posts, or that they frequently link to "fake news" sites? While this is not digital redlining because it is not based on zip code, it feels similarly underhanded. People expect lending decisions to be made on directly

128. In fact, Facebook has patented technology that would purportedly allow "lenders to use a borrower's social network to determine whether he or she is a good credit risk." *See* Ananya Bhattacharya, *Facebook Patent: Your Friends Could Help You Get a Loan—or Not*, CNN (Aug. 4, 2015, 6:58 PM), http://money.cnn.com/2015/08/04/technology/facebook-loan-patent [https://perma.cc/F3CR-K7XW].

129. *See* Robinson Meyer, *Could a Bank Deny Your Loan Based on Your Facebook Friends?*, ATLANTIC (Sept. 25, 2015), https://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287 [https://perma.cc/NP2A-XKZM] ("Since one's friends so closely mirror one's race and class—according to one study, nine out of 10 of the average white American's friends are also white—the practice would effectively restore loan discrimination.").

relevant information—credit histories, salaries, and the like. On the other hand, lending decisions made based on a user's Facebook posts or friend network are not only unexpected, but could also unfairly discriminate against certain populations. In the worst-case scenario, it could be a way for a lender to get around antidiscrimination law by using proxies for race. If it could be proven that this practice had disparate impact on minority borrowers, it would likely be discriminatory and in contravention of Facebook's fiduciary duty.

C. LIMITED SHARING WITH THIRD PARTIES[130]

Discrimination and manipulation both focus on what a company might do internally that would disregard a user's reasonable expectations or violate the user's trust. A third concern is more external-facing: to whom can a fiduciary disclose a user's data?[131] Service providers often have privacy policies in which they identify third parties with whom they share user information. But in some cases, sharing personal information may be a violation of trust: users may have shared data based on their relationship with and confidence in Company A, which does not extend to Company B. The users might not have disclosed that information in the first place if they had known Company B would have access to it; in this way, sharing takes away users' agency and choice over who accesses their data. But beyond the user's distrust of Company B, Company A's act of sharing her personal data changes the relationship between the user and the

130. This Article explicitly focuses on consumer privacy in the private marketplace. Much has been written—and remains to be written—on the government's usage of data and on private firms sharing data with the government. *Carpenter v. United States*, for example, a case heard by the Supreme Court in October Term 2017, will address the warrantless search of cellphone records that indicate the user's location and movements over several months. Carpenter v. United States, 137 S. Ct. 2211 (2017) (granting certiorari). But this Article leaves government data collection to be dealt with separately. In order to focus on the heart of the information fiduciary duty, the author has chosen to avoid complicating the analysis by introducing a host of other laws and standards which are necessarily at play in government data collection. That said, the government should also have to abide by certain standards in data collection and usage.

131. This Article focuses on voluntary disclosure or sale of data. Hacking is also a concern. However, for the purpose of this Article, it suffices to say that a company may also breach its fiduciary duty by not securing data properly, or not notifying users promptly when a hack has occurred. *See, e.g.*, Greg Bensinger & Robert McMillan, *Uber Reveals Data Breach and Cover-Up, Leading to Two Firings*, WALL ST. J. (Nov. 21, 2017, 11:38 PM), https://www.wsj.com/articles/uber-reveals-data-breach-and-cover-up-leading-to-two-firings-1511305453 [https://perma.cc/24CA-W94W]. Because hacking is generally not purposeful on the part of the hacked firm, it does not fall into the category of things the company could do affirmatively to breach its duty.

company; once Company A shares a user's personal data, the user's trust in the company has been undermined.[132]

The identities of third parties with whom service providers may share information varies widely from provider to provider. From a user's point of view, some of these likely seem reasonable—for example, that Facebook shares the information a user posts with their selected audience (most likely their friend network), and that Uber shares a user's information with drivers. However, some of this sharing is less predictable, such as Uber's sharing of information with "vendors, consultants, marketing partners, research firms, and *other service providers or business partners*."[133] This last category is disturbingly vague, especially because it is clear that this portion of the policy refers to personally identifiable information. The list *later* references aggregated data (which Uber may share with any third parties, according to its policy), indicating that the earlier provision applies to non-aggregated, or personally identifiable information.[134]

1. Identities and Obligations of Third Parties

In considering a fiduciary duty for service providers, it is important to decide with which third parties data can be shared consistent with users' expectations. For the purposes of this Article, third parties are defined as companies other than the end-user and the service provider with whom the end-user directly interacts. It is difficult to identify every type of third party and categorize whether a service provider who wants to maintain fiduciary status can give them data. Circumstances change, and users' expectations of Uber, for example, may be different than their expectations of Facebook or Walmart. However, there are a few rules of thumb that may help define "third parties." In all cases, a company that receives user data from a service provider must immediately become an information fiduciary to the individuals included in the dataset, and thus comply with all responsibilities of the original fiduciary. In no situation should a service provider share data with a company that does

132. *Cf.* Morgan Hochheiser, Comment, *The Truth Behind Data Collection and Analysis*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 32, 52 (2015) ("Selling data exploits a consumer and therefore is against public policy. The public needs to trust businesses and the government, but if businesses sell private information and the government allows it, the public has no one to trust with their PII.").

133. *Privacy Policy*, UBER (Sept. 21, 2017), https://privacy.uber.com/policy [https://perma.cc/4K8M-7TWW] (emphasis added).

134. *Uber Privacy Statement 2015*, UBER (July 15, 2015), https://d3i4yxtzktqr9n.cloudfront.net/privacy-policy/static/past-policies/privacy-policy-2015-en-1244ec7107.pdf [https://perma.cc/4KDN-H6TJ] ("We may share your information . . . [i]n an aggregated and/or anonymized form which cannot reasonably be used to identify you.").

not uphold an information fiduciary duty; doing so knowingly would be a violation of the company's own duty as well.

Subsidiaries of the same holding company and "partners" are often recipients of user data. Sharing of user information with these kinds of recipients should be allowed when it enhances the service being provided—not merely when it "helps business" in some vague way. For example, Waze Mobile,[135] whose parent company is Alphabet, Inc., should be able to share data with Google Maps, since the integration of traffic data is part of the service that users appreciate and on which they rely. However, many companies are subsidiaries of holding companies which parent several seemingly unrelated businesses. For example, Alphabet also owns Zagat,[136] a company that rates restaurants, and Nest,[137] a company that makes smart-home thermostats.[138] Users may not expect that by using Zagat's phone app, they are providing data that may be shared with Nest and Waze. Whether this sharing violates the fiduciary duty should be determined case-by-case based on whether a reasonable user would have expected it.

Advertisers are often third parties as well. While targeted advertising is a necessary component of many business models, it does not require that individual user data be shared with advertisers. Instead, advertisers should identify groups they want to target (for example, women between the ages of twenty to thirty who have expressed an interest in a particular television show, activity, food, and so on), and the service provider should identify the actual targets. While targeted advertising as a phenomenon is often in users' interests since it keeps the cost of services down by generating higher advertising revenues, there is no need for individuals' information to be shared with advertisers to make this business model work. As such, it would be inconsistent with a fiduciary duty to share user information with third parties.

An additional third party is trackers—companies who provide analytical tools to websites that want to collect or utilize user data. Fifteen percent of

135. Darrell Etherington, *Google's Waze Acquisition Bears First Fruit As Mobile Google Maps App Gets Real-Time Incident Reports*, TECHCRUNCH (Aug. 20, 2013), https://techcrunch.com/2013/08/20/googles-waze-acquisition-bears-first-fruit-as-mobile-google-maps-app-gets-real-time-incident-reports/ [https://perma.cc/F8V4-EGTT].

136. ZAGAT, https://www.zagat.com [https://perma.cc/RG73-KYYY] (last visited Feb. 28, 2018).

137. NEST, https://nest.com [https://perma.cc/BAL9-ZATX] (last visited Feb. 28, 2018).

138. Mike Murphy & Akshat Rathi, *All of Google's—er, Alphabet's—Companies and Products from A to Z*, QUARTZ (Aug. 10, 2015), https://qz.com/476460/here-are-all-the-alphabet-formerly-google-companies-and-products-from-a-to-z [https://perma.cc/4STQ-H46L].

global websites share private data to ten or more tracker operators.[139] Facebook and Google are the biggest providers of tracking tools, though a number of companies offer them.[140] These companies are essential to websites that want to benefit from data collection. But as third-party recipients of data, they should bear the same fiduciary responsibilities as the primary website with which the user interacts. For example, the Mayo Clinic website uses a number of trackers; it also allows users to learn about HIV tests and make appointments.[141] The Mayo Clinic should have a fiduciary obligation with regard to that data, and so should the third-party tracker that the Clinic uses.

Another potential third party with which data can be shared is an aggregator, such as Acxiom, a company that, as of 2013, owned about 1,500 data points[142]—including "household income, ZIP code, race, ethnicity, social network or interests like 'smoking/tobacco' or 'gaming-casino' "[143]—on 700 million individuals.[144] Aggregators collect data from thousands of sources and aggregate fuller profiles on individual users, presenting a host of problems for fiduciaries. Users conceive of their relationships with various companies as separate from each other; when a user tells Facebook that she enjoys cooking, she does not expect Blue Apron, Stop & Shop, or Amazon/Whole Foods to be able to purchase a list with her name and email address. But an aggregator can match her email address with Google searches to identify how often she searches for recipes or her Facebook profile to show that she often posts photos of food. The aggregator can then sell that much more valuable profile to any number of companies.

But Acxiom and companies like it cannot be information fiduciaries to anyone—the fiduciary relationship requires that users know a company is collecting their data and that users have placed some sort of trust in that company. Users do not willingly give their data to companies like Acxiom; "consumers are often unaware of the existence of data brokers as well as the purposes for which they collect and use consumers' data."[145] So when

139. *See* GHOSTERY, *supra* note 57.

140. *See* Macbeth, *supra* note 6, at 5-6.

141. *See* GHOSTERY, *supra* note 57.

142. Katy Bachman, *Confessions of a Data Broker*, ADWEEK (Mar. 25, 2014), http://www.adweek.com/digital/confessions-data-broker-156437 [https://perma.cc/SD74-G3MG].

143. Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. Times (Feb. 27, 2015), https://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html [https://perma.cc/6XHM-MU26].

144. Bachman, *supra* note 142.

145. Press Release, Fed. Trade Comm'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), https://www.ftc.gov/news-events/press-

aggregators create this fuller profile, often facilitating discrimination and manipulation, users are unaware of its existence. For this reason, no fiduciary should be able to share data with a company whose business model is built on collecting data from many sources and selling fuller profiles, and no fiduciary should be able to purchase and/or utilize data collected by one of these companies.

Data can be shared in an identifiable format or in an aggregated format. The discussion above covers the sharing of identifiable information. Sharing aggregated data with third parties is consistent with an information fiduciary duty if no individual is personally identifiable and there are no unique identifiers for any one person.[146] Aggregated datasets may help companies provide better service without posing much risk of harm to individuals. If a company aggregates data to identify products that are preferred by a certain demographic group or to determine usage behavior by certain groups or at certain times, that information could help their business without breaching any individual's trust. But if the aggregated data is used to discriminate against or manipulate users—thus violating the principles outlined above—it would still violate the fiduciary duty.

One could argue that even aggregated data-sharing can be harmful. For example, what if a company discovers and publicizes that a certain age and racial group is particularly susceptible to cigarette advertisements, encouraging tobacco companies to target those people? Many people might see this as a negative outcome, but it must be separated from the principle of data privacy. No individual's privacy has been breached, and the company has not breached its fiduciary duty. An argument that the company did not use those individuals' data in their best interest would also require companies to make judgments about which products are "good" and which are "bad." Companies should be able to be neutral in their data sharing; we should allow Facebook to aggregate and sell a report about exercise trends and smoking trends because the law should not be making those kinds of judgments through privacy policy.

releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data [https://perma.cc/N2US-T7DG].

146. For example, it should not be possible for two companies to create a unique identifier system such that their datasets are easily combined and individuals become identifiable.

2. Hypotheticals

a) Uber Broadcasts the Locations of Well-Known People at a Launch Party

As mentioned in Part I, Uber projected the real-time location of Peter Sims, an angel investor, on a wall during their Chicago launch party.[147] The third party here is not someone who would buy the data to enhance their own business; here, Uber shared an individual's data with a third party (the party attendees) to market its product. This violates the company's fiduciary duty by breaching the user's trust; the sharing did not enhance the service for Sims—in fact, as he explained, it weakened it—and it was certainly unexpected. After Sims learned from a friend that Uber had displayed his location and the location of other "NYC certain 'known people,' . . . I expressed my outrage to her that the company would use my information and identity to promote its services without my permission. She told me to calm down, and that it was all a 'cool' event and as if I should be honored to have been one of the chosen. What nonsense."[148]

But if Uber had just displayed the location of one hundred anonymous celebrities, there might be no way to determine which celebrities were being tracked. This could be consistent with the fiduciary duty if no individual's data were traceable back to them. Merely displaying the data in real-time on a wall does not leave much room for disaggregation, and because no rider is identifiable, Uber could be within its rights to do this.

b) Facebook Tells Someone's Friends About Their Purchases

Facebook and other platforms are integrated with many other sites. When users buy something from a clothing store's website, they can often sign into that website using their Facebook logins, which then grants Facebook varied levels of access to their interactions with the clothing website. Facebook may know what items users purchased, and could then present their friends with advertisements (presumably in concert with the store) that display the items and mention that a friend purchased it. This could be potentially embarrassing; what if it is a personal item about which you would not have told your friends, such as a self-help book, a particular medication, or a financial product? But that does not mean it is inconsistent with the fiduciary duty. First of all, when a user provides her Facebook username and password to log into another website, there is a pop-up that explains what data will be available to whom.

147. Sims, *supra* note 1.
148. *Id.*

The notification, in its current form, is typically short and clear[149] and may be enough to shift a reasonable user's expectations of the companies involved.[150] The resulting third-party sharing should, then, be within the user's expectations; trusting Facebook to *not* use or share this data once a user has been warned would be unreasonable.[151]

But shift the hypothetical so that Facebook advertises the items someone has purchased to strangers, with a note that provides her name and says she has purchased the items. This situation is more difficult. The difference lies in how a user conceives of Facebook. The website exists for the purpose of sharing information about your life with the outside world, but Facebook leads users to believe that with the right privacy setting, only a users' "friends" can see information about them. Because Facebook sets up this expectation, it would be a violation of the resulting trust for Facebook to share purchase information with a non-friend (that is to say, someone whom the user has not approved for access to their posts). The average Facebook user expects that when they have the option to adjust privacy settings so that only friends can view their information, the website will act in accordance with those settings.

c) Uber Uses Data To Embarrass a Critic

In 2014, an Uber executive suggested—perhaps off-handedly—that in order to fight negative press stories accusing Uber of sexism and misogyny, Uber should hire opposition researchers and use the data it has about a particular journalist to "give the media a taste of its own medicine."[152] Uber's then-CEO, Travis Kalanick, maintained that this was a departure from Uber's "values and ideals,"[153] but the suggestion is interesting—could it do this and remain within a fiduciary duty?

149. One such notification reads, "This app may post on your behalf, including radio stations you joined, songs you played and more." Whitson Gordon, *Understanding OAuth: What Happens When You Log into a Site with Google, Twitter or Facebook*, LIFEHACKER (June 13, 2012, 1:00 PM), https://lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook [https://perma.cc/VU8S-UWM3].

150. See Part IV for further discussion on shifting user expectations.

151. There is also a question about manipulation here—is it manipulative to use my friends to advertise to me? However, this is the kind of practice with which consumers are familiar. It is essentially an even more sophisticated level of targeted advertising, but users likely understand what is happening and do not lose autonomy when it occurs.

152. Ben Smith, *Uber Executive Suggests Digging Up Dirt On Journalists*, BUZZFEED (Nov. 17, 2014, 4:57 PM), www.buzzfeed.com/bensmith/uber-executive-suggests-digging-up-dirt-on-journalists [https://perma.cc/CN3K-MPAP].

153. Josh Constine, *Uber CEO Says Exec's Threats To Journalists "Showed A Lack Of Humanity" But Doesn't Fire Him*, TECHCRUNCH (Nov. 18, 2014), https://techcrunch.com/2014/11/18/emil-michael-thrown-under-the-uber [https://perma.cc/KK4F-RVD6].

Consider a case in which Uber targets a particular critic and looks through the data they have gathered through the journalist's use of the service. Uber finds that she is married with two children, and lives with her husband and family in Brooklyn. However, her Uber data shows her leaving work, going to the same Upper West Side apartment several nights a week, and then heading back to her own home after a few hours. This, paired with data that shows the apartment belongs to a male work associate of hers, could suggest she is having an affair. The next time the journalist writes a column criticizing Uber, Uber responds with a blog post describing her affair in an effort to discredit her.

Assuming Uber is targeting the one journalist and not a specific class of people, its actions do not violate the principle of antidiscrimination. But this would violate the third-party principle through the sharing of data in a completely unexpected way. While Uber is not releasing a spreadsheet of data, it is presenting the user's data (i.e., the journalist's ride history) in a public story about her. Under no circumstance would a reasonable user expect her data to be used in this way.

Additionally, Uber is using her data to manipulate her in two ways. If the story is published on Uber's blog, it is manipulative first because Uber is attempting to covertly push an agenda—one that is aimed at discrediting a journalist.[154] If someone from Uber publishes the story without attaching Uber's name, the increased covertness makes it more manipulative. Second, this is a usage of a user's data to maximize the company's own welfare by bringing down a critic, at the expense of the journalist's privacy and reputation. As such, this kind of behavior crosses multiple lines which violate the fiduciary duty. To be clear, it is the usage of the data, which the user provided to Uber to facilitate a specific service that makes this action a violation of Uber's fiduciary duty. If Uber had merely written a blog post discrediting the journalist by pointing to other stories she had written, picking on her lackluster education, or just fabricating lies, it would not violate its informational fiduciary duty because it would not be using information it possessed by virtue of the journalist having used Uber's service.

D. VIOLATING THE COMPANY'S OWN PRIVACY POLICY

The final principle, which prohibits firms from violating their own privacy policies, does not just define a fourth aspect of the information fiduciary duty. It also illuminates the underlying assumption of the information fiduciary duty itself—that users' reasonable expectations mark the ultimate limit on data privacy practices. Thus, if practices are brought within users' expectations or are predictable to a reasonable user, the practice will not violate the fiduciary

154. This violation might be remedied if the story makes clear that this journalist has been critical of Uber—the agenda-pushing would no longer be covert.

duty. As mentioned in Section II.A, the FTC routinely uses its Section 5 authority to hold companies accountable to the standards they set for themselves in their privacy policies. But ultimately, companies should not be able to set their own standards—there should be some baseline to which every service provider is held.[155] Though the FTC is empowered to bring enforcement actions based on the policies,[156] baseline standards are needed.

Most companies' privacy policies discuss with whom data may be shared. The policies vary widely, but almost all allow some sort of sharing with other companies. Notably, the typical privacy policy highlights sharing, but not internal company practices. This indicates that service providers may not believe they should have to disclose to users how they use data internally or what practices they will and will not implement.[157]

---

155. Of course, firms should be permitted to provide *more* protection that the information fiduciary baseline.

156. 15 U.S.C. § 45 (2012); *see also supra* Section II.A.

157. Walmart, which claims it "cares deeply about maintaining the trust and confidence that our customers place in us," *Responsible Disclosure Policy*, WALMART, https://corporate.walmart.com/article/responsible-disclosure-policy [https://perma.cc/PJ9Y-8HA6] (last visited Feb. 28, 2018), says only that the company "will not sell or rent your personal information" but may "share your personal information in limited circumstances, such as to conduct our business, when legally required, or with your consent." *Walmart Privacy Policy*, WALMART (Nov. 2017), http://corporate.walmart.com/privacy-security/walmart-privacy-policy [https://perma.cc/RYD5-ADLA].

Uber's policy says that it may share information with: (1) drivers; (2) other riders if a ride-sharing service is used; (3) other people as directed by the user; (4) the general public if the user submits content in a public forum; (5) the owner of Uber accounts that someone uses (i.e., their employer); (6) Uber subsidiaries, affiliates, service providers, and business partners; (7) "law enforcement officials, government authorities, or other third parties as necessary to enforce our Terms of Service, user agreements, or other policies, to protect Uber's rights or property or the rights or property or others"; (8) third parties to provide a service requested by the user through a partnership or promotional offering; (9) Uber "vendors, consultants, marketing partners, research firms, and other service providers or business partners"; (10) in connection with or during merger negotiations; or (11) if consent is given. UBER, *supra* note 134.

Google's privacy policy maintains that it does not share personal information outside Google unless: (1) they have the user's consent, which is opt-in for sensitive personal information; (2) the information is being shared with domain administrators; (3) the information is being shared for external processing; or (4) the information is being shared for legal reasons. The policy further articulates that Google may share non-personally identifiable information with "partners," which includes publishers, advertisers, and connected sites. *Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy [https://perma.cc/56MF-W2L6].

Facebook's policy says it shares information with: (1) "people you share and communicate with"; (2) people that see content others share about you; (3) apps, websites, and third-party integrations on or using Facebook's services; (4) Facebook companies; and (4) a new owner,

1. An Information Fiduciary's Privacy Policy

An information fiduciary must comply with the restrictions it imposes on itself, because that is the promise it has made to its users. But a user's expectations of a company can be shifted through clear disclosures.[158] When a company makes a promise in its privacy policy, such as that it "will not sell or rent your personal information,"[159] it must not violate that promise. As discussed, the FTC and CFPB have sued companies for misrepresentation when they have violated their own privacy policies.[160] One could argue that a user's expectations cannot be based on privacy policies, since users never read them. However, if the fiction works in *favor* of service providers, in that they are allowed to continue various practices if they have "disclosed" them, the fiction should also be extended to protect users.

But in an ideal (and hopefully not-too-distant) world, privacy policies could be one to two pages, and easy to read and comprehend.[161] In that case, it is even more important that companies abide by their own policies since users may actually be able to make informed decisions when engaging with a company. An information fiduciary should be required to provide clear disclosures that identify the company's data privacy policies in plain language. Key practices might be those which are most pervasive or those which are least predictable. A good model is the CFPB's "Know Before You Owe" mandatory one-page disclosure for mortgage loans.[162] The CFPB performed research for

---

if an acquisition were to occur. Additionally, though, Facebook shares non-personally identifiable information with "advertising, measurement, and analytics services" and vendors, service providers, and "other partners who globally support our business." *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php [https://perma.cc/Q64D-FF4T] (last visited Feb. 28, 2018).

158. This also indicates that one of the previous four mandates can be circumvented through clear disclosure.

159. *Walmart Privacy Policy*, WALMART, *supra* note 157.

160. *See, e.g.*, Press Release, Fed. Trade Comm'n, Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices (Dec. 20, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively [https://perma.cc/4V5T-VW3B].

161. *Cf.* KLEIMANN COMMC'N GRP., INC., KNOW BEFORE YOU OWE: QUANTITATIVE STUDY OF THE CURRENT AND INTEGRATED TILA-RESPA DISCLOSURES (2013), https://s3.amazonaws.com/files.consumerfinance.gov/f/201311_cfpb_study_tila-respa_disclosure-comparison.pdf [https://perma.cc/LZB6-KA5K] (describing the development of the CFPB's mortgage disclosure rules); KLEIMANN COMMC'N GRP., INC., KNOW BEFORE YOU OWE: EVOLUTION OF THE INTEGRATED TILA-RESPA DISCLOSURES (2012), https://s3.amazonaws.com/files.consumerfinance.gov/f/201207_cfpb_report_tila-respa-testing.pdf [https://perma.cc/5PJL-KU5G] (describing the study that informed the drafting of the mortgage disclosure form design).

162. *See Know Before You Owe: Mortgages*, CONSUMER FIN. PROT. BUREAU 1 (Nov. 20, 2013), http://files.consumerfinance.gov/f/201311_cfpb_factsheet_kbyo_mortgage-disclosures.pdf

over two years to determine how to make disclosures most helpful to consumers.[163] Information fiduciaries should provide a similar type of form rather than the thousands of words of small, light grey text that many provide now. This would allow a user to understand how their data might be used and decide accordingly whether to hand over their information. To be sure, service providers should not be able to disclaim certain duties, such as the duty not to covertly manipulate, but they could notify users of other practices and allow users to then decide for themselves about whether they want to use the service.

2. Hypothetical: Facebook Pushes a Political Agenda, Part II

Think back to an early hypothetical, in which Facebook pushed a political agenda on users. What if when users signed up for the service Facebook disclosed that it may push its political agenda on users? Or if Facebook sent every current user an email alerting them to the implementation of a new practice? This might make it consistent with the fiduciary duty. The reason that manipulation of a user's autonomy is unacceptable is because it is covert, so users cannot respond to it rationally and consciously. If Facebook tells users that it will try to get them to vote a certain way, the "manipulation" is now more like targeted advertising—the user is able to respond to it.

A natural reaction to this might be that people stop using Facebook. But would they? Facebook's network effects are immense; many users might just go along with it, as they have with a number of companies that have publicly implemented unsavory policies. As Albert Hirschman explains, users can respond to a company's change in policies in two ways: exit or voice.[164] If exit is difficult, users can respond with voice. And the decision between these two options will be affected by how loyal the user feels to the company.[165]

[https://perma.cc/47TK-57XF] (hereinafter CFPB, *Mortgages*) ("The two new forms, one which consumers will receive shortly after applying for a loan and one which they will receive shortly before closing, use plain language and design to make it easier for consumers to locate key information such as the interest rate, monthly payments, and the costs to close the loan."); *see also How We Improved the Disclosures*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/know-before-you-owe/compare [https://perma.cc/QGU4-4YGP] (last visited Feb. 28, 2018).

163. CFPB, *Mortgages*, *supra* note 162, at 2.

164. *See generally* ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970). "Exit" represents the idea that, when management has "failed," consumers can stop buying the firm's products, causing revenue to drop. *Id.* at 4. The other option that consumers can use to express displeasure, "voice," occurs through "general protest addressed to anyone who cares to listen." *Id.*

165. *Id.* (explaining that were loyalty is lacking, people would be more likely to choose exit over voice).

Exit and voice have worked for users in this space. For example, in 2012, Instagram changed its policy to claim the right to sell users' photos.[166] Within two days, there was so much backlash that Instagram retreated from the policy.[167] So Facebook—or any other service provider—does have the option to push an agenda if it is out in the open, and they may or may not risk user exit. And smaller companies with fewer network effects may simply have to implement a privacy policy that is acceptable to its potential users.

IV. ENFORCING THE INFORMATION FIDUCIARY DUTY

Simply defining practices that may or may not be consistent with an information fiduciary duty is not enough. There are two main paths forward from here—one involving legal changes and the other involving industry changes. On the legal side, two steps must be taken to make the information duty a reality: (1) a federal statute that imposes the duty on service providers, and (2) enforcement in courts.[168] While this Article does not purport to lay out a new statutory scheme in its entirety, it briefly sketches out what this might look like in practice.

The statute would define this duty and categorize who is subject to it. The main task would be to define "service provider" to state clearly who must abide by the information fiduciary duty. Coverage should be clear and predictable for industry. Ideally, it would cover any company that collects user data and stores it beyond the conclusion of each transaction, with some sort of exception for firms that serve a small number of users.[169] But outside of defining the category of covered entities and the general duty, the statute should be general. Courts could define its contours as cases arise by determining what a "reasonable user" should expect. The duty itself is based on users' expectations, which will shift as data collection practices, artificial

166. *See* Joshua Brustein, *Anger at Changes on Instagram*, N.Y. TIMES (Dec. 18, 2012, 4:05 PM), https://bits.blogs.nytimes.com/2012/12/18/anger-at-changes-on-instagram [https://perma.cc/26W9-8U5Z].

167. *See* Harold Maass, *Instagram's Privacy Policy Retreat: Too Late?*, WEEK (Dec. 21, 2012), https://theweek.com/articles/469195/instagrams-privacy-policy-retreat-late [https://perma.cc/VR42-UJFV]; *see also* Nicole Perlroth & Jenna Wortham, *Instagram's Loss Is a Gain for Its Rivals*, N.Y. TIMES (Dec. 20, 2012, 10:00 PM), https://bits.blogs.nytimes.com/2012/12/20/instagrams-loss-is-other-apps-gain [https://perma.cc/ATJ4-Z58C].

168. States could do this as well but because of the complications stemming from data territoriality and the fact that many service providers serve consumers in all fifty states, a federal regime would be more predictable for users and service providers alike.

169. This would likely require a study to determine what constitutes a "small business" in the online service provider and data collection space, but should end up falling in line with other small business exceptions, to avoid undue burden.

intelligence, and the Internet of Things continue to develop and change the way users interact with technology and the world more broadly.

A broad statute that allows courts to easily adapt it to users' changing expectations is not as unpredictable as it sounds. A statute should define the fiduciary duty as maintaining data collection and usages practices that are consistent with a reasonable user's expectations. Judges are well-versed in defining the "reasonable person," and juries are asked to do it all the time.[170] Consider a hypothetical lawsuit against Facebook for manipulating users by pushing a political agenda. A judge or jury would look at all of the facts and determine whether a reasonable user should have expected this manipulation.

The proposed California Consumer Privacy Act of 2018 is an interesting model for this kind of legislation.[171] While it does not specifically propose a fiduciary duty, it takes a number of steps to level the playing field between users and service providers such that users have the ability to understand more fully how data is collected and used. For example, it requires businesses to disclose what personal information it has collected to individual consumers upon request[172] and gives users the right to prevent businesses from selling their personal information.[173]

Once a fiduciary duty is legally imposed, it could be enforced privately or publicly. California's proposed law provides for both avenues.[174] The concern with private enforcement would be defining an injury-in-fact such that the threat of private litigation has an effect on companies' behavior.[175] It is a viable mechanism, but public enforcement is likely a stronger tool. The FTC and state agencies should be given an active role in enforcing this law to ensure that it does not go unenforced simply because of standing doctrine.

---

170. *See, e.g.*, People v. Jefferson, 14 Cal. Rptr. 3d 473, 481 (Cal. Ct. App. 2004) ("The jury must consider defendant's situation and knowledge, which makes the evidence relevant, but the ultimate question is whether a reasonable person, not a reasonable battered woman, would believe in the need to kill to prevent imminent harm."); State v. Morgan, 648 N.W.2d 23, 32–33 (Wis. Ct. App. 2002) (defining the reasonable person in the context of *Miranda* analysis); Radtke v. Everett, 501 N.W.2d 155, 166 (Mich. 1993) (defining the standard and maintaining that "the reasonable person standard is sufficiently flexible . . . without destroying the vital stability provided by uniform standards of conduct"); *see also* Alan D. Miller & Ronen Perry, *The Reasonable Person*, 87 N.Y.U. L. REV. 323 (2012) (arguing that normative definitions of the "reasonable person" are preferable to positive definitions).

171. THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018, VERSION 2 (Oct. 12, 2017), https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf [https://perma.cc/HK5A-S6NM].

172. *Id.* § 1798.101.

173. *Id.* § 1798.102.

174. *Id.* §§ 1798.108 to 1798.109.

175. This is the subject of much debate, *see, e.g.*, Spokeo v. Robins, 136 S. Ct. 1540 (2016), but is outside the scope of this Article.

But while the law should impose this duty, the beauty of the fiduciary duty lies in the ability to shift user expectations. An additional step that should be taken is for companies to take privacy policies more seriously—not just as a liability issue, but as an opportunity. Rather than bury provisions in thousands of words of small, light grey text, companies could produce one-page policy summaries that define key terms and describe data practices. By doing so, a "reasonable user's" expectations should shift, and the company can test or implement new practices. By allowing users a meaningful chance to opt in or out, companies could allow them to act autonomously and see what users are willing to allow. Companies should enable their users to engage with them on equal footing so that ultimately, users can make informed decisions about how they share their data.

V. CONCLUSION

The United States has a long way to go in terms of mandating protections for users' personal information. Holding service providers to an information fiduciary standard is a viable way to ensure that data-focused business models can continue to function while individuals are adequately protected. The four principles outlined here—anti-manipulation, antidiscrimination, limited third party sharing, and holding companies to their own privacy policies—all focus on user expectations. And as new technologies emerge and old tools morph into something new, user expectations may change.

As Justice Sotomayor noted in 2012, "[p]erhaps . . . some people may find the tradeoff of privacy for convenience worthwhile, or come to accept this diminution of privacy as inevitable, and perhaps not."[176] As people become more comfortable with emerging technologies, their "reasonable expectations" may shift. But shifting expectations should not be an excuse for a complete lack of privacy standards for firms. There can be a tradeoff that works for the service provider and the user, and if the standard is based in reasonableness, it can evolve alongside technology. Abiding by fiduciary principles will help service providers be the trustworthy entities they hold themselves out to be, ensuring that the era of Big Data does not necessarily mean the end of personal privacy.

176. United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (internal quotations omitted).