UC DAVIS LAW REVIEW

VOL. 49, NO. 4 APRIL 2016

Information Fiduciaries and the First Amendment

Jack M. Balkin[*]

TABLE OF CONTENTS

 Knight Professor of Constitutional Law and the First Amendment, Yale Law School. This Essay is based on remarks delivered at the Central Valley Foundation/James B. McClatchy Lecture on the First Amendment at UC Davis School of Law on March 12, 2015. My thanks to the members of the UC Davis faculty; to Yochai Benkler, Jane Birnbaum, Andrew Gold, James Grimmelmann, Neil Richards, and Jonathan Zittrain for their comments and suggestions about the ideas presented in this Essay; and to Christina Krushen and Luke Maher for research assistance.

INTRODUCTION

Collection, analysis, and use of personal data increasingly affect everything we do in the information age, from our personal privacy to our opportunities for jobs, housing, travel, and health care. As algorithms for making decisions based on this data become more powerful, so too will the people and organizations who collect and use the data.

Reformers will press for government regulation in the name of protecting personal privacy and preventing abuse and discrimination. In response, businesses that collect, analyze, use, distribute, and sell personal data will likely raise First Amendment defenses. It will only be natural for them to try to prevent what they regard as meddlesome and invasive government regulation by invoking the First Amendment — one of the most central of our constitutional liberties.

These developments are part of a far larger trend in which the First Amendment has gradually been transformed into a bulwark of protection against business regulation. This is not the first time such a transformation has occurred. The American Civil War was fought, among other things, over the rights of free labor, which were then understood as equally central to civil liberty and equality of citizenship.[1] During the first Gilded Age, the right of free labor — now reinterpreted as a right of freedom to contract — became an important constitutional defense against new forms of economic regulation.[2]

The New Deal reconstituted the concept of civil liberties, and the First Amendment rights of speech, press, and association became the paradigmatic examples of constitutional liberty. Now, in our second

---

[1] *See generally* ERIC FONER, FREE SOIL, FREE LABOR, FREE MEN: THE IDEOLOGY OF THE REPUBLICAN PARTY BEFORE THE CIVIL WAR (1970).

[2] *See* Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 26 (2004) [hereinafter *Digital Speech and Democratic Culture*] ("Courts turned the ideology of free labor into a constitutional principle of liberty of contract that prevented governments from regulating wages and working conditions."); *see, e.g.*, Allgeyer v. Louisiana, 165 U.S. 578, 589 (1897) (holding that the liberty protected by the Due Process Clause of the Fourteenth Amendment includes the right "to pursue any livelihood or avocation" and "to enter into all contracts which may be proper" for these purposes). For accounts of how Gilded Age ideas of freedom of contract were created out of Jacksonian and free labor ideals, see, for example, Michael Les Benedict, *Laissez-Faire and Liberty: A Re-Evaluation of the Meaning and Origins of Laissez-Faire Constitutionalism*, 3 LAW & HIST. REV. 293 (1985); William E. Forbath, *The Ambiguities of Free Labor: Labor and the Law in the Guilded Age*, 1985 WIS. L. REV. 767, 798-99; Charles W. McCurdy, *The Roots of "Liberty of Contract" Reconsidered: Major Premises in the Law of Employment, 1867–1937*, *in* YEARBOOK 1984: SUPREME COURT HISTORICAL SOCIETY 20 (1984).

Gilded Age, the First Amendment has become the most fertile source of constitutional defenses to business regulation.[3]

I find myself on both sides of this emerging conflict. On the one hand, I understand that human freedom in the information age requires regulation of new forms of social and economic power, just as it did in the first Gilded Age. On the other hand, I also believe in the constitutional freedoms of the First Amendment. This essay attempts to make these two commitments cohere — to show how protections of personal privacy in the digital age can co-exist with rights to collect, analyze, and distribute information that are protected under the First Amendment.

In this essay, I reconcile these seemingly opposed interests through the concept of an *information fiduciary*.[4] This concept describes an important category of people and businesses in the digital age. I will argue that many online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users.

Because of their special power over others and their special relationships to others, 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. These duties place them in a different position from other businesses and people who obtain and use digital information. And because of their different position, the First Amendment permits somewhat greater regulation of information fiduciaries than it does for other people and entities.

Not all information fiduciaries are the same, however; the duties they take on depend on the nature of their business and the reasonable expectations of the public. Equally important, not everyone on the

[3] Balkin, *Digital Speech and Democratic Culture*, *supra* note 2, at 25 ("One of the most important developments of the past quarter century is the emergence of the First Amendment and the free speech principle as anti-regulatory tools for corporate counsel."); *id.* at 27-28 (describing features of a Second Gilded Age, in which "[f]reedom of speech is becoming a generalized right against economic regulation of the information industries" and "[p]roperty is becoming the right of the information industries to control how ordinary people use digital content"); J.M. Balkin, *Some Realism About Pluralism: Legal Realist Approaches to the First Amendment*, 1990 DUKE L.J. 375, 383-85 (predicting a "transformation" and "ideological drift" in free speech doctrine and explaining that "[b]usiness interests . . . are finding that arguments for property rights . . . can more and more easily be rephrased in the language of the first amendment by using the very same absolutist forms of argument offered by the left in previous generations" (internal quotation marks omitted)).

[4] Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [hereinafter *Information Fiduciaries*].

Internet is an information fiduciary, and the First Amendment rights of these actors are unaffected by the analysis I offer here. My goal, in other words, is to shift the focus of First Amendment arguments about privacy from the kind of *information* to the kinds of *relationships* — relationships of trust and confidence — that governments may regulate in the interests of privacy.

The concept of information fiduciaries does not solve all of the problems that lie at the intersection of information privacy and the First Amendment. And it does not solve all of the problems of overreaching that will inevitably occur in the age of Big Data. Even so, it helps us better understand a wide range of issues. I will also point out how the concept of information fiduciaries should cause us to rethink some of our doctrines of Fourth Amendment law, another part of the Constitution concerned with information privacy.

I. TWO STORIES ABOUT DATA

To explain some of the central problems that digital privacy presents for standard First Amendment doctrines, I begin with two stories. The first is about Uber, an online car service. The second is about Facebook, the popular social media site.

In November 2014, BuzzFeed revealed that a senior executive at Uber, Emil Michael, was furious at the negative coverage of the company by a journalist, Sarah Lacy. Michael suggested at a dinner — in front of reporters no less! — that the company might hire opposition researchers to gather and spread embarrassing details about Lacy's personal life.[5]

Of course, Uber does not need to hire private investigators if it wanted to embarrass or coerce people. It sits on a gold mine of private information about its users. Uber knows when people take rides, where they are coming from, where they are going to, their location during each part of the ride, and the time the rides begin and end.

In addition, Uber executives have revealed the existence of software features — sometimes called a "God View" — that allow real-time tracking of drivers, of riders, and of people waiting for rides.[6] Uber has

[5] Ben Smith, *Uber Executive Suggests Digging Up Dirt on Journalists*, BUZZFEED (Nov. 17, 2014, 5:57 PM), http://www.buzzfeed.com/bensmith/uber-executive-suggests-digging-up-dirt-on-journalists.

[6] Johana Bhuiyan & Charlie Warzel, *"God View": Uber Investigates Its Top New York Executive for Privacy Violations*, BUZZFEED (Nov. 18, 2014, 8:27 PM), http://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy; Kashmir Hill, *'God View': Uber Allegedly Stalked Users for Party-Goers' Viewing Pleasure (Updated)*, FORBES (Oct. 3, 2014, 11:32 AM), http://www.forbes.com/sites/kashmirhill/

strenuously denied that it is misusing this information.[7] In theory, however, Uber might use this data in lots of different ways to embarrass journalists, politicians, or other people who use the service. In theory, for example, Uber could reveal information suggesting that customers were engaged in extramarital affairs or engaged in secret or illegal meetings that they would not want others to know about.

This is not merely speculation. An Uber executive who was meeting with a journalist read the journalists' location logs and sent them to her to see why she was late. The company later disciplined the executive for the use of the data.[8]

Moreover, companies like Uber and the dating site OkCupid understand that people are fascinated by Big Data and what companies can now do with all of the data they collect. People like to hear about all the interesting inferences that data scientists can draw about our collective behavior. Accordingly, OkCupid has published stories about what data tells us about users' sexual practices,[9] while Uber has used its data to print interesting stories about the people who use its services and how they use them. For example, in a blog post entitled "Rides of Glory," Uber explained how to use the data it collects to tell if someone is using Uber to travel to and from a one-night stand.[10]

My second story comes from Harvard's Jonathan Zittrain, and it is about Facebook.[11] Facebook wanted to know if it could encourage people to vote, so it decided to perform an experiment on its users.

2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/.

[7] Bhuiyan & Warzel, *supra* note 6.

[8] *Id.*; Lisa Vaas, *Uber: We Accessed Reporter's Private Trip Info Because She Was Late*, NAKED SECURITY (Dec. 17, 2014), https://nakedsecurity.sophos.com/2014/12/17/uber-we-accessed-reporters-private-trip-info-because-she-was-late/; Letter from Katherine Tassi, Uber Managing Counsel — Privacy, to Senator Al Franken, *available at* http://www.franken.senate.gov/files/documents/141215UberResponse.pdf (last visited Feb. 17, 2016).

[9] Christian Rudder, *10 Charts About Sex*, OKTRENDS (Apr. 19, 2011), http://blog.okcupid.com/index.php/10-charts-about-sex/ ("All the data below, even the most personal stuff, has been gleaned from real user activity on OkCupid. Some of it our users have told us outright by answering match questions; some of it we've had to learn from observation.").

[10] Derrick Harris, *The One-Night Stand, Quantified and Visualized by Uber*, GIGAOM (Mar. 26, 2012, 4:05 PM PST), https://gigaom.com/2012/03/26/uber-one-night-stands/. Uber's blog post on "Rides of Glory" has since been taken down, in the wake of the disclosure of Uber's God View. *See* Chanelle Bessette, *Does Uber Even Deserve Our Trust?*, FORBES (Nov. 25, 2014, 5:36 PM), http://www.forbes.com/sites/chanellebessette/2014/11/25/does-uber-even-deserve-our-trust/. The post, however, is still available on the Internet Archive. Voytek, *Rides of Glory*, UBER BLOG (Mar. 26, 2012), https://web.archive.org/web/20140827195715/http://blog.uber.com/ridesofglory.

[11] Jonathan Zittrain, Response, *Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy*, 127 HARV. L. REV. F. 335, 335-36 (2014), http://

In the Facebook feeds of tens of millions of its users, the company placed a graphic with a link for looking up the nearest place to vote, the profile photos of up to six Facebook friends who had indicated they had already voted, and a button for the end-user to announce that he or she had voted.[12] The idea was to encourage people to vote by showing them that their friends had voted.[13] Other Facebook users in the experiment were simply shown a generic message urging them to vote.[14] Then Facebook cross-referenced its end-users' names with publicly available voting records to measure how much the special voting prompt increased turnout over the generic message.[15]

It turns out that users who were told that their friends had voted were 0.39 percent more likely to vote than those who received a generic get out the vote message.[16] Moreover, once they posted a message saying that they had voted, they tended to influence their own Facebook friends, even if the latter had not received the special message.[17] The researchers concluded that the graphic directly added 60,000 votes that would otherwise not have been cast, and the ripple effect may have added an additional 280,000, for a total of 340,000 votes.[18]

Zittrain then asks: What if Facebook decided to use its power to influence elections? Facebook can use personal data to predict who a user is likely to support.[19] Suppose Facebook decided that it wanted a candidate of a certain party to win, and so it sent voting prompts to people likely to support that candidate in close races, like the Florida race in the 2000 presidential election that was decided by a mere 537 votes.[20] Zittrain calls this practice "digital gerrymandering" and argues that it should not be legal.[21]

Note the differences between the two stories. The danger in the Uber story is that the company might use sensitive personal data to

harvardlawreview.org/2014/06/engineering-an-election/ [hereinafter *Engineering an Election*]; Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [hereinafter *Facebook Could Decide an Election*].

12 Zittrain, *Engineering an Election*, *supra* note 11, at 335.

13 *Id.*

14 Zittrain, *Facebook Could Decide an Election*, *supra* note 11.

15 *Id.*

16 *See id.*

17 *Id.*

18 *See id.*

19 *Id.*

20 *Id.*

21 *Id.*

embarrass or otherwise harm its users. The problem in the Facebook story is different. Facebook is not trying to embarrass or harm its users. It just wants to experiment on them, whether for the advancement of science, for profit, or (potentially) for political advantage.

How does the First Amendment fit in? Are these activities protected because they involve the collection, analysis, use, sale, and distribution of data?

First, consider the Uber example. Eugene Volokh has argued that many privacy laws regulating the sale and disclosure of personal information are unconstitutional under existing First Amendment law.[22] These privacy protections attempt to create a right to keep people from saying things about you — especially true things.[23] Such laws, Volokh argues, presumptively violate the First Amendment, and we cannot escape the First Amendment by asserting that they are merely matters of private concern.[24]

If so, then Uber's disclosure of sensitive personal information about its users might be protected by the First Amendment unless it also attempted to threaten users or blackmail them. (Blackmail and threats, of course, are not protected by the First Amendment.[25]) To be sure, Uber might conceivably have violated the privacy tort of disclosure of true embarrassing facts.[26] But many commentators argue that the tort is on constitutionally shaky ground, and that its scope should be construed as narrowly as possible to avoid serious First Amendment problems.[27] Uber might argue, accordingly, that disclosures tending to

[22] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000).

[23] *See id.* at 1050-51 ("[T]he right to information privacy — my right to control your communication of personally identifiable information about me — is a right to have the government stop you from speaking about me.").

[24] *Id.* at 1089 (arguing that the claim that governments may regulate speech of private concern to protect information privacy "is theoretically unsound . . . precedentially largely unsupported . . . [and] has proven unworkable; and, if adopted, it would strengthen the arguments for many other (in my view improper) speech restrictions").

[25] *See, e.g.*, Virginia v. Black, 538 U.S. 343, 359 (2003) ("'true threats'" unprotected); Watts v. United States, 394 U.S. 705, 707 (1969) (same).

[26] *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977). The tort of disclosure allows civil liability when the defendant "gives publicity to a matter concerning the private life of another," when the "matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Id.*

[27] *See, e.g.*, Volokh, *supra* note 22, at 1088-95 (arguing that basing privacy

undermine the credibility of a journalist who is criticizing Uber's practices should be considered newsworthy and beyond the reach of the tort.[28]

Companies in Uber's position can do many things short of overt threats or blackmail that might worry people. A company like Uber might simply want to embarrass its critics, and other people would quickly get the message that it is unwise to cross the company. Uber might also want to raise additional revenue by selling locational data to other companies who want to predict consumer behavior about things that have nothing to do with transportation services.

Volokh's argument suggests that all of these disclosures and sales are speech about a person and that, with a few limited exceptions, the First Amendment protects them.[29] Of course, all this assumes that the information is true. If the information sold or disclosed to others is false and defamatory, the answer would be different, although companies might still be protected to some extent under the constitutional privileges recognized in *New York Times Co. v. Sullivan*[30] and *Gertz v. Robert Welch, Inc*.[31] But privacy regulation usually seeks to do more than prevent common-law defamation.

In *Sorrell v. IMS Health Inc.*,[32] the Supreme Court struck down regulations that sought to limit the communication and distribution of personal data about doctors. Vermont was concerned that pharmacies were selling information about doctor prescriptions to data miners, who in turn sold reports about doctors' prescribing tendencies to

regulation on the identification of non-newsworthy matters of private concern is theoretically unsound and will lead to other improper speech restrictions); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 294 (1983) (noting the "serious constitutional problems" with the tort of disclosure of true private facts). Volokh points out that one might treat differently cases of *exposure* — in which pictures of people are presented naked, or on the toilet, or in undignified situations. Volokh, *supra* note 22, at 1094.

[28] *See, e.g.*, Shulman v. Group W Prods., Inc., 955 P.2d 469, 478 (Cal. 1998) ("[L]ack of newsworthiness is an element of the 'private facts' tort," making newsworthiness a complete bar to common law liability); *cf.* § 652D cmt. d (1977) ("When the subject-matter of the publicity is of legitimate public concern, there is no invasion of privacy.").

[29] Volokh, *supra* note 22, at 1122.

[30] 376 U.S. 254, 279-80 (1964) (holding that defamation against public officials is protected unless made with actual malice).

[31] 418 U.S. 323, 347-49 (1974) (holding that statements of opinion are constitutionally protected and that the *New York Times* privilege applies to public officials and public figures but not to private figures).

[32] 131 S. Ct. 2653 (2011).

pharmaceutical companies and their detailers (salesforce).[33] The state's concern was that allowing drug companies to target advertising at doctors would cause doctors to prescribe more expensive drugs.[34] Hence, Vermont made it illegal for pharmacists to sell information about doctor prescriptions for marketing purposes.[35] *Sorrell* held the regulation unconstitutional because it was a content-based and speaker-based restriction on access to information and on speech employed for marketing purposes.[36] Justice Kennedy's majority opinion pointed out that under Vermont's law, pharmacists could donate or sell the same information to other parties for scientific, journalistic, or other purposes.[37]

Justice Kennedy strongly suggests that the creation, sale, and dissemination of personal information in the form of data can claim protection as speech under the First Amendment.[38] But he found it unnecessary to decide the question because even if collections of data were unprotected, Vermont's law discriminated on how people and organizations could use the data in communications on the basis of content and speaker.[39] These restrictions violated the First Amendment, even under the intermediate scrutiny tests used for commercial speech.[40]

Next, consider Jonathan Zittrain's Facebook example. The problem in this case is not so much that Facebook is disclosing information about the targets of its experiment, although the company did disclose to end-users that other Facebook friends voted.[41] Rather, the problem is that Facebook is manipulating its end-users by dividing them into segments and sending targeted messages to particular groups to get them to act in certain ways. Moreover, the danger is that Facebook

[33] *Id.* at 2659-60.

[34] *Id.* at 2661.

[35] *Id.* at 2662-63.

[36] *Id.* at 2663, 2667 ("The State has imposed content- and speaker-based restrictions on the availability and use of prescriber-identifying information. So long as they do not engage in marketing, many speakers can obtain and use the information. But detailers cannot.").

[37] *Id.* at 2668.

[38] *Id.* at 2667 ("This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment.").

[39] *Id.* (noting that because the statute involved "content- and speaker-based restrictions on the availability and use of prescriber-identifying information . . . . this case can be resolved even assuming, as the State argues, that prescriber-identifying information is a mere commodity").

[40] *Id.* at 2667-68.

[41] Zittrain, *Engineering an Election*, *supra* note 11, at 335.

might manipulate people based on their likely political affiliation in order to further Facebook's interests.

But here too, we might say, all of this activity is protected by the First Amendment. In fact, what Facebook is doing is political speech. Urging someone to go and vote is core political speech;[42] indeed, it is about as central to the core of the First Amendment as anything else. And urging many people to vote should be just as protected as urging one person to vote.

If we treat what Facebook did as a scientific experiment, then it might claim a First Amendment right to engage in the speech necessary to perform the experiment and to collate the information (which is available publicly) to measure the results of the experiment. One might object that if Facebook were part of a university it might have to bring its proposed experiment before a human subjects review board. But Facebook is not part of a university.[43]

Moreover, if the real complaint is that Facebook's message urging people to vote is selectively targeted, why should this matter from the standpoint of the First Amendment? Much digital advertising these days is targeted;[44] people receive different messages depending on what Facebook or Google knows about them. Surely the First Amendment protects the right of people to choose who they will and will not speak to. Moreover, political advertising that uses e-mail is also regularly targeted. It does not lose First Amendment protection for this reason. Nor can the problem be that the targeting works to the

[42] *See, e.g.*, Mills v. Alabama, 384 U.S. 214, 215, 220 (1966) (striking down criminal ban on newspaper publishing "an editorial on election day urging people to vote a certain way on issues submitted to them").

[43] For a discussion of some of the ethical problems, see James Grimmelmann, *The Law and Ethics of Experiments on Social Media Users*, 13 COLO. TECH. L.J. 219, 255-58 (2015), describing the phenomenon of "IRB Laundering," in which social scientists can use private companies to perform experiments on human subjects without having to conform to university regulations for human subjects research.

[44] *See, e.g.*, JOSEPH TUROW, BREAKING UP AMERICA: ADVERTISERS AND THE NEW MEDIA WORLD (1997) (offering a history of targeted advertising from the 1970s to the beginning of the digital age); JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH (2011) (describing techniques of digital marketing in the twenty-first century); *As Brands Turn to Digital Advertising to Reach the Right Audience, Focus on Validation Is Increasing*, FORBES (May 5, 2015, 9:00 AM), http://www.forbes.com/sites/forbespr/2015/05/05/as-brands-turn-to-digital-advertising-to-reach-the-right-audience-focus-on-validation-is-increasing/ ("Currently, 90% of companies spend at least 25% of their digital advertising budgets on specific targets, and 43% of companies spend more than half of their budgets reaching specific targets. Most (84%) of companies expect that investment to increase.").

advantage of Facebook. Targeted advertising is supposed to benefit the commercial or political advertiser; that fact does not rob the advertising of First Amendment protection.[45]

It would seem to follow, then, that the First Amendment puts rather strict limits on how government might regulate companies, like Uber and Facebook, that collect large amounts of information about end-users and then analyze, use, distribute, and sell that information to make profits, or to gain business or political advantages.

Is this true? Is there really no way to regulate these practices consistent with the First Amendment? Consider some possible legal theories.

II. SOME POSSIBLE FIRST AMENDMENT SOLUTIONS

A. Distinguishing Between Collection, Analysis, Use, Disclosure, and Sale

At the outset, we should distinguish between different kinds of information practices, each of which may be treated differently under the First Amendment. In particular, we should distinguish (1) collection, (2) analysis, (3) use, (4) disclosure, and (5) sale of information.[46] The Uber and Facebook stories are primarily about disclosure and use of personal information, although these are made possible by collection and collation. The First Amendment protects some of these activities differently than others. In particular, privacy regulations might face fewer First Amendment problems when they focus on the *collection* and *use* of data rather than on the analysis, disclosure, and sale of data that is otherwise lawfully in one's possession.[47]

We should not, however, conclude too hastily that there are no First Amendment rights to collect information. Courts are beginning to recognize a First Amendment right to record events that take place in public.[48] Early cases have focused on citizens' rights to record police

[45] *See, e.g.*, Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976) ("[T]hat the advertiser's interest is a purely economic one . . . . hardly disqualifies him from protection under the First Amendment.").

[46] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1181-82 (2005) (offering a similar taxonomy).

[47] *See id.* at 1182 (noting that collection and use rules are usually treated differently from restrictions on disclosure and sale).

[48] *See, e.g.*, ACLU of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012) (holding that the right to make "an audio or audiovisual recording is necessarily included within the First Amendment's guarantee of speech and press rights as a corollary of the right to disseminate the resulting recording"); Glik v. Cunniffe, 655 F.3d 78, 83

officers or other government officials in public settings,[49] but the logic might be extended to any events that occur in public.[50] A right to record might conceivably protect a wide range of technologies for collection of public information, with the limiting case being harassment and violations of the tort of intrusion on seclusion.[51] As camera-equipped drones come into common use, courts, legislators, and regulators alike are increasingly confronted with constitutional limits on collection of data.[52]

The scope of a right to record is beyond the scope of this essay. I note merely that if there is a right to collect information in public through digital or analogue recording, there might also be a right to collect information in the form of data.[53] Imagine that instead of Uber or Facebook, members of the press collected the data, collated the information, and presented the results in a newspaper account. Unless we can come up with plausible distinctions between the right to record data in digital form (which is what a cellphone does) and the right to collect data, the First Amendment may treat both the same.[54]

(1st Cir. 2011) ("[T]he First Amendment protects the filming of government officials in public spaces."); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000) ("The First Amendment protects the right to gather information about what public officials do on public property, and specifically, a right to record matters of public interest."). *But cf.* Kelly v. Borough of Carlisle, 622 F.3d 248, 262-63 (3d Cir. 2010) (holding that the right to record is not clearly established for purposes of qualified immunity doctrine). *See generally* Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIRCUIT 57, 62-63 (2013) (discussing circuit decisions on the right to record).

[49] *See, e.g.*, *Glik*, 655 F.3d at 79 (recognizing right to record public officials in public spaces); Gilles v. Davis, 427 F.3d 197, 212 n.14 (3d Cir. 2005) (citing *City of Cumming*, 212 F.3d at 1333) (noting that "videotaping or photographing the police in the performance of their duties on public property may be a protected activity"); *City of Cumming*, 212 F.3d at 1333 ("The First Amendment protects the right to gather information about what public officials do on public property, and specifically, a right to record matters of public interest."); Robinson v. Fetterman, 378 F. Supp. 2d 534, 541-42 (E.D. Pa. 2005) (basing the right to record police officers on the fact that "[t]he activities of the police, like those of other public officials, are subject to public scrutiny").

[50] *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 84-86 (2014) (explaining why the right to collect and create information suggests a broad right to record); Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 409 (2011) ("[T]he First Amendment protects the right to record images we observe as part of the right to form, reflect upon, and share our memories.").

[51] *See* Bambauer, *supra* note 50, at 63-64, 111-12; Kreimer, *supra* note 50, at 397-98.

[52] *See* Kaminski, *supra* note 48; Kreimer, *supra* note 50, at 404-06.

[53] For a sustained argument to this effect, see Bambauer, *supra* note 50, at 85.

[54] *See, e.g.*, *id.* at 83 ("In time, the rule that mechanically capturing information is

The most obvious difference is that data collected on a public street using a cell phone seems "public" and therefore part of public discussion. By contrast, personal data collected on the Internet seems "private" and not a contribution to public discourse. The problem I am interested in is how to make sense of that distinction.

B. Data as Commodity or as Speech

One might argue that data, when collected, collated, used, and sold in bulk, is not speech at all. Rather, it is a commodity, like widgets or soybeans. Vermont made this argument in *Sorrell*; although the Court did not decide the question, Justice Kennedy's majority opinion seemed skeptical.[55] Yet it is not clear that the *format* in which information is delivered is the crucial distinction. If a journalist or scientist published data in the course of a report to the public, it should be protected speech. Instead of focusing on the *form* of information as digital data, we may need to focus instead on its *social characterization* or *social function*.

C. Privacy Regulations as Time, Place, and Manner Regulations

We might also argue that privacy regulations are content-neutral regulations of time, place, and manner of expression. We might rely on *Bartnicki v. Vopper*,[56] in which both the majority and the dissent agreed that restrictions on disclosure of intercepted material without consent were content-neutral time, place, and manner regulations.[57] *Bartnicki* also seems to suggest, however, that there is a right to distribute information on matters of public concern, lawfully obtained, to the public.[58] Hence, if one wants to control disclosure or sale, one still has to show that the information collected in the course of business is not a matter of public concern.[59] The time, place, and

nonexpressive conduct will prove to be unworkable.").

[55] Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011); *see also* Bambauer, *supra* note 50, at 71-72.

[56] 532 U.S. 514 (2001).

[57] *Id.* at 526 (stating that "the communications at issue are singled out by virtue of the fact that they were illegally intercepted — by virtue of the source, rather than the subject matter" or the content); *id.* at 544 (Rehnquist, C.J., dissenting, joined by Scalia & Thomas, JJ.) (agreeing that the regulations were content-neutral).

[58] *See id.* at 535 (holding that if a reporter lawfully obtained material about a matter of public concern, the First Amendment protects the right to communicate it even if it was originally obtained illegally).

[59] *See, e.g.*, Trans Union Corp. v. FTC, 267 F.3d 1138, 1140-41 (D.C. Cir. 2001) (noting that speech on matters of private concern may warrant less constitutional

manner theory, in other words, does not answer the central issue: how to distinguish between information that can be made part of public discourse and information that can be kept out of public discourse. Nevertheless, as *Bartnicki* itself suggests, once we figure out how to define matters of private concern, the time, place, and manner approach to privacy makes considerable sense. Moreover, it may explain constitutional privacy regulations directed to collection or to use rather than to sale or disclosure.

On the other hand, the time, place, and manner approach seems to require content neutrality. First Amendment problems may arise if governments direct privacy regulations only at particular classes of businesses, restrict only the commercial marketing of data, or restrict only the use of data for advertising purposes. *Sorrell* subjected speaker-selective privacy regulations to heightened scrutiny; it also held that restrictions aimed only at marketing would be vulnerable.[60] And a recent case, *Reed v. Town of Gilbert*,[61] seems to suggest that even innocuous subject matter restrictions may prevent municipal regulations from being content-neutral.[62]

D. Commercial Speech

Still another solution would be to treat regulations of the collection, analysis, use, disclosure, and sale of data as regulations of commercial speech, which receives somewhat less protection than other speech.[63] This approach has a superficial plausibility because it is mostly

protection and can be regulated in the interests of privacy).

[60] *Sorrell*, 131 S. Ct. at 2667.

[61] 135 S. Ct. 2218 (2015).

[62] *Compare id.* at 2228-30 (explaining that laws that distinguish among signs based on their content, including their subject matter, are "subject to strict scrutiny regardless of the government's benign motive, content-neutral justification, or lack of 'animus toward the ideas contained' in the regulated speech" (quoting City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 429 (1993))), *with id.* at 2236-37 (Kagan, J., concurring, joined by Ginsburg & Breyer, JJ.) (describing wide range of sign ordinances that are now subject to strict scrutiny under the new doctrine).

[63] Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 477 (1989) ("Our jurisprudence has emphasized that 'commercial speech [enjoys] a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values,' and is subject to 'modes of regulation that might be impermissible in the realm of noncommercial expression.'" (quoting Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978))); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 562-66 (1980) (setting out a four-part test for commercial speech regulation which imposes intermediate scrutiny and permits regulation of misleading speech and speech which advocates illegal commercial activity).

commercial entities who collect, use, and sell personal data, and the sale of data is a commercial transaction. But this is not a solution; it is a play on words.[64] Commercial speech is speech whose social function is to encourage commercial transactions; the central example is commercial advertising.[65] The fact that a commercial entity engages in speech does not make it commercial speech; otherwise, every article in the *New York Times* would be commercial speech. And the fact that data is bought and sold in bulk by commercial enterprises does not make it commercial speech either. Otherwise, books and music bought and sold in bulk by commercial enterprises would be commercial speech.

To be sure, restrictions on the collection, analysis, use, distribution, and sale of personal data may *also* violate the right to engage in commercial speech. That is because government restrictions may hamper the ability of businesses to target potential customers and fashion customized messages.[66] But the more basic question is whether the collection, analysis, use, distribution, or sale of personal data — whether or not helpful to commercial advertising — is protected by the First Amendment.[67]

Although some personal data is sold, much of it is not; often it is kept and used by the business that collects it, for purposes that go well beyond advertising. For example, in the two stories that begin this essay, Uber and Facebook were not offering to sell their data to others; they were using the data for internal purposes. Nor were they using the data to advertise products to their end users.[68]

Equally important, the commercial speech strategy is premised on the assumption that it will be considerably easier for governments to secure information privacy if courts treat data as commercial speech. Yet *Sorrell* suggests that a majority of the Justices will offer true and non-misleading commercial speech protection almost as great as core political speech.[69] Thus, if the data that companies are collecting,

---

[64] *See* Volokh, *supra* note 22, at 1080-81.

[65] *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976) (holding that the Constitution protects "speech which does 'no more than propose a commercial transaction'" (quoting Pittsburgh Press Co. v. Pittsburgh Comm'n, 413 U.S. 376, 385 (1973))).

[66] *See* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1232-33 (10th Cir. 1999) (determining that restrictions on the sale of consumer data about telephone customers was a restriction on commercial speech because it interfered with telephone company's ability to target customers for advertising purposes).

[67] *See* Bambauer, *supra* note 50, at 73-74.

[68] *See supra* Part II.

[69] *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2663-64 (2011) (applying

analyzing, using, and selling is accurate, calling it commercial speech will not be of much help.

E. Contract

Eugene Volokh has argued that we can protect privacy by private ordering through contract.[70] Parties can agree contractually to information privacy rules. *Cohen v. Cowles Media Co.*[71] suggests that contracts not to disclose are enforceable, even against journalists who are engaged in core exercises of protected speech. *Cowles Media* applied promissory estoppel against a journalist who caused a source to rely on his assertion that he would not disclose the source's identity.[72]

Volokh's point is that although the state may not be able to keep you from saying things to others that you do not like, it can enforce private contracts that achieve the same goal.[73] To the extent that companies promise not to collect, analyze, use, sell, or disclose personal data in particular ways, the First Amendment will not protect them if they violate their promises. Thus, we can hold companies like Uber or Facebook to the terms of the privacy policies stated in their end-user license agreement or terms of service.

However, the flip side of the contract theory is that if there is no contract (or reliance-inducing promise), there is no constitutionally enforceable privacy right. And because companies like Uber and Facebook can state their privacy policies in vague terms, or change their privacy policies more or less at will, relying on terms of service or end user license agreements may offer only very limited privacy protections.

The contractual solution to the balance between First Amendment and privacy regulation is similar to a property model of privacy. The contract solution treats personal privacy as an entitlement that end-users may consent to surrender or transfer to companies, with the default rule being that in the absence of an agreed-to privacy policy, consumers have no right to control information that they have voluntarily provided to companies. The First Amendment then respects the result of whatever bargain is reached.

"heightened judicial scrutiny" to Vermont's law because it made content- and speaker-based distinctions); *id.* at 2677-79 (Breyer, J., dissenting, joined by Ginsburg & Kagan, JJ.) (arguing that majority has imported features of First Amendment doctrine that apply to core speech into commercial speech doctrine).

70 Volokh, *supra* note 22, at 1057-63.

71 501 U.S. 663 (1991).

72 *Id.* at 668-72.

73 *See* Volokh, *supra* note 22, at 1057-58, 1061-62.

Many privacy scholars have pointed out that relying solely on this approach to privacy protection will seriously under-protect people's privacy. People are not very good at privacy management; they do not understand the cumulative effects of their agreements to allow collection, analysis, use, and sale of information about them.[74]

Moreover, Daniel Solove and Woodrow Hartzog have pointed out that "contract law — formal contract and promissory estoppel — plays hardly any role in the protection of information privacy, at least vis-à-vis websites with privacy policies."[75] Attempts to use privacy policies to protect consumer privacy have generally met with failure, and much consumer privacy regulation has fallen to administrative agencies like the Federal Trade Commission ("FTC").[76]

F. The Limits of the Contractual Model

The contract model has other shortcomings. Paul Schwartz has pointed out that it does not seem to account for widely accepted privacy practices in highly regulated areas like health care.[77] How does one explain, for example, the traditional duties of confidentiality between doctors and patients, the increasingly elaborate privacy regulations of electronic patient records, or the fracturing of health care services into multiple institutions? Modern health care privacy law is largely a set of government created regulations, rather than a result of private ordering.[78]

---

[74] *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1149 (2011) ("Many consumers have little idea how much of their information they are giving up or how it will be used."); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502 (2000) ("[C]onsumers suffer from privacy myopia: they will sell their data too often and too cheaply."); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1452 (2001) ("It is difficult for the individual to adequately value specific pieces of personal information."). Information and learning costs often deter effective contracting. *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 341, 360-61 (Jane K. Winn ed., 2006) (noting that privacy policies are often difficult to understand and therefore most Americans do not read them).

[75] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 596 (2014).

[76] *Id.* at 596-97.

[77] Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1565-66 (2000) (noting that freedom of contract solutions are not well-equipped to deal with contemporary use of medical records).

[78] *Id.*

Volokh offers a possible solution: he suggests that implied contracts for privacy should be as enforceable as explicit contracts.[79] He argues that doctors and patients, even without explicitly making promises, or entering into negotiations, reasonably expect that patient information will be kept confidential because of customary practice.[80] In this way one might bring traditional doctor-patient and lawyer-client relationships within the contractual model.

Yet this does not really solve the problem. First, customs can and do change over time, and they change when people explicitly reject or alter them. Thus, a theory of implied contract does not protect people if doctors specifically alter patient expectations by announcing that patients should not expect that their information will be kept confidential.[81] There are good reasons why doctors may not do this (which I will discuss momentarily), but they are more about tort than contract.

Second, in modern health care, patients have relationships not only with their doctors but with a wide range of institutions, from hospitals to health maintenance organizations to insurers, and it is difficult to see how one could plausibly describe privacy obligations in terms of implied contracts with all of them. Indeed, patients may not have any contracts or agreements with some of them.[82]

Third, to the extent that the implied contract theory depends on well-understood and longstanding customs that generate reasonable expectations of how health care professionals and patients will interact, it is unlikely to be helpful in deciding how and whether to extend privacy protections to new kinds of health care providers or entities that collect and process health care records.[83] Indeed, as noted above, health care privacy is primarily regulated by public law, not contract law; governments impose health privacy regulations on many

[79] Volokh, *supra* note 22, at 1057-58 ("In many contexts, people reasonably expect — because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract — that part of what their contracting partner is promising is confidentiality." (footnote omitted)).

[80] *Id.*

[81] Volokh argues that "a legislature may indeed enact a law stating that certain legislatively identified transactions should be interpreted as implicitly containing a promise of confidentiality." But this only acts as a default rule, and would not apply if "such a promise is explicitly and prominently disclaimed by the offeror, and the contract together with the disclaimer is accepted by the offeree." Volokh, *supra* note 22, at 1060.

[82] Schwartz, *supra* note 77, at 1565-67; *see* Volokh, *supra* note 22, at 1059-60 (noting difficulty of assessing expectations of confidentiality in a wide range of situations).

[83] *See* Schwartz, *supra* note 77, at 1566-67.

different kinds of actors, as the federal government does in the Health Insurance Portability and Accountability Act ("HIPAA")[84] and other statutes. The contractual model would place all of these arrangements — even the most sensible — in jeopardy of constitutional challenge.

The contractual model of privacy protection, in short, begs some of the most important questions about privacy regulation. For example, the state might decide that businesses should have certain kinds of privacy policies; or it might add or imply privacy guarantees in contracts between businesses and end-users.[85] Sometimes the state might impose privacy protections as default rules; but sometimes it might impose terms that the parties cannot easily contract around. A contract model suggests that some or all of these practices may be vulnerable under the First Amendment, at least to the extent that the parties have not explicitly or implicitly agreed to these state-mandated terms.[86]

Indeed, a contractual model of privacy has an interesting feature. It tends to conflate First Amendment freedom with contractual freedom. Conversely, it creates potential First Amendment problems for all forms of state privacy regulation that cannot be cashed out in terms of enforcing private contracts. To the extent that information privacy regulation is achieved through private contract, it is presumptively constitutional under the First Amendment. But if the state attempts to regulate information privacy contracts by rewriting important terms, or by imposing unwaivable duties, the regulation may be constitutionally suspect under the First Amendment.[87] In this way, the contract model

[84] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[85] To give only one recent example, in September 2014, California enacted the Student Online Personal Information Protection Act ("SOPIPA"), which restricts how Internet and cloud-based sites, applications, and services designed for K–12 educational purposes can use student data; and prevents these entities from selling, using, or distributing student data for targeted marketing purposes. *See* Student Online Personal Information Protection Act (SOPIPA), CAL. BUS. & PROF. CODE § 22584(a)–(b)(4) (2016).

[86] *See* Volokh, *supra* note 22, at 1061-62 (describing limits of contractual approach). Volokh does not claim that contractual approaches to privacy will give privacy advocates everything they would like. His point, rather, is that "contractual solutions are a constitutional alternative and may be the only constitutional alternative, not that they are always a particularly satisfactory alternative." *Id.* at 1062.

[87] For example, in the Telecommunications Act of 1996, Congress imposed a duty of "confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers." 47 U.S.C. § 222(a) (2012). Congress permitted carriers to use customer information within the confines of the existing service relationship, but prohibited carriers from otherwise using, disclosing or allowing access to such information "[e]xcept as required by law or with the approval of the customer." *Id.* § 222(c)(1).

brings back Lochnerian premises in an unexpected way. By connecting the boundaries of what the First Amendment permits and forbids to the exercise of contractual liberties, it in effect turns First Amendment protections into protections of freedom of contract.

A 1999 decision, *U.S. West, Inc. v. FCC*,[88] offers an example. In the Telecommunications Act of 1996, Congress directed telecommunications facilities to protect consumer privacy.[89] In order to enforce Congress's mandate, the Federal Communications Commission ("FCC") issued regulations concerning the collection and sale of customer proprietary network information ("CPNI") — that is, data about consumers' activities on the phone network.[90] The FCC imposed "opt-in" rules, which assumed that consumers wanted privacy protection, and therefore required express prior customer consent for most carrier uses of consumer data.[91] U.S. West preferred an "opt-out" rule, which allowed it to use and sell the data unless the consumer expressly said "no."[92] The 10th Circuit agreed with U.S. West that attempting to shift the default rule violated the First Amendment.[93] On remand, the Commission adopted more lenient "opt-out" rules, which allowed carriers to use CPNI in most instances, provided that customers received notice in advance and had an opportunity to refuse consent or "opt out."[94]

U.S. West is not the last word. In 2009, in *National Cable & Telecommunications Ass'n v. FCC*,[95] the D.C. Circuit upheld new FCC rules that imposed opt-in requirements against a First Amendment challenge.[96] It assumed that Congress could constitutionally impose a

---

[88] U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

[89] *See supra* note 87.

[90] *U.S. West*, 182 F.3d at 1228 & n.1.

[91] *See id.* at 1230.

[92] *See id.* at 1240, 1246-47 (Briscoe, J., dissenting).

[93] *Id.* at 1239 (majority opinion) ("Even assuming that telecommunications customers value the privacy of CPNI, the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy.").

[94] Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996, 998-99 (D.C. Cir. 2009) (summarizing FCC rulemaking following *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999)).

[95] *Id.*

[96] *Id.* at 999-1000 (upholding 2007 rules that required carriers "obtain opt-in consent from a customer before disclosing that customer's [information] to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related services to that customer" (citation omitted) (internal quotation marks omitted)). In an earlier case involving the Fair Credit Reporting Act, the D.C. Circuit also held that opt-out rules were not required by the First Amendment as a less restrictive alternative to regulation of commercial speech. *See*

duty on telecommunications carriers to protect the privacy of their customers, and it held that opt-in rules were a reasonable means of achieving consumer privacy.[97]

These two privacy cases exemplify a basic problem for contractual models of privacy. Contractual models require a fairly administrable distinction between contractual protections of privacy — which, generally speaking, do not raise First Amendment problems — and tort causes of action for invasion of privacy — which often do.[98] The difficulty, as every professor of private law knows, is that the boundaries between contract and tort are fuzzy.

Governments may want to protect consumer privacy by adding default rules, implying duties, and adding state-imposed terms and obligations to consumer privacy contracts. Shifting entitlements through default rules may be acceptable under the contractual model if the default rules are clearly stated at the outset and easy to contract out of.[99] But the more difficult it becomes to change privacy protections by contract, the more the contractual obligation looks like a tort duty imposed by the state. And when the state imposes non-waivable duties — by statute or by administrative regulation — it is essentially offering a tort theory of privacy protection. Then the contractual theory of privacy protection will not be of much help.[100] In *National Cable & Telecommunications Ass'n*, the D.C. Circuit upheld statutory and administrative privacy regulations against First Amendment challenge by treating the sale of consumer data as commercial speech and then holding that the regulations passed intermediate scrutiny.[101] But, as noted above, although data may help

Trans Union Corp. v. FTC, 245 F.3d 809, 811, 818-19 (D.C. Cir. 2001) (upholding FTC enforcement pursuant to the Fair Credit Reporting Act that limits the ability of companies to sell lists of names and addresses of consumers to target marketers).

97 *Nat'l Cable & Telecomms. Ass'n*, 555 F.3d at 1000-02.

98 *See* Volokh, *supra* note 22, at 1061 (noting that the disclosure tort cannot be justified under the contract theory); *see also* Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989) (holding that a state may not punish publication of "lawfully obtain[ed] truthful information about a matter of public significance . . . absent a need to further a state interest of the highest order" (quoting Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979)) (internal quotation marks omitted)).

99 *See* Volokh, *supra* note 22, at 1060 (noting that shifting defaults may be constitutional under these conditions).

100 *Id.* at 1061 ("*Cohen v. Cowles Media* cannot validate speech-restrictive terms that the government compels a party to include in a contract; the case at most validates government-specified defaults that apply unless the offeror makes clear that these terms aren't part of the offered deal.").

101 *See Nat'l Cable & Telecomms. Ass'n*, 555 F.3d at 1000-02; *see also Trans Union Corp.*, 245 F.3d at 818-19.

advertisers engage in commercial speech, the sale and distribution of the underlying data is not really commercial speech.[102]

III. INFORMATION FIDUCIARIES

I certainly do not mean to suggest that we should simply give up on all of the approaches I have just described. We may be able to modify or elaborate some of them so that they offer an appropriate level of privacy protection. But in this essay, I want to suggest another way of approaching the problem — through the idea of fiduciary duties. The idea of fiduciary duties gives us a way out of the neo-Lochnerian model that binds First Amendment freedoms to contractual freedom. It also offers us a way of explaining why certain kinds of information are *matters of private concern* that governments can protect through reasonable regulation.[103] My central point is that certain kinds of information constitute matters of private concern not because of their *content*, but because of the *social relationships* that produce them.[104]

Suppose that a doctor, lawyer, or accountant sold personal information about their clients to a data broker. Suppose that they used personal information to manipulate a client's actions for the doctor, lawyer, or accountant's benefit. Or suppose that they simply disclosed it in order to gain a business advantage at the expense of their client. If they did any of these things, they would likely be liable for a violation of professional conduct, which courts might characterize either as a breach of a duty of professional obligations or as professional malpractice.[105] These torts normally occur in the

---

[102] *See supra* text accompanying notes 63–69.

[103] *See, e.g.*, *supra* notes 56–59 and accompanying text (discussing *Bartnicki v. Vopper*).

[104] This builds on an important point about the contractual model that people may overlook. What the contractual model gets right is that what makes privacy obligations enforceable notwithstanding the First Amendment is not the content of the speech but a legally enforceable social relationship; namely, contract. But other kinds of legally enforceable social relationships — namely, fiduciary relationships — may have the same effect.

[105] Some courts and commentators treat a breach of professional or fiduciary duty (which includes a duty of confidentiality) as a tort separate from professional malpractice, arguing that malpractice primarily concerns duties of care, whereas breach of fiduciary duty is primarily about a duty of loyalty. *See, e.g.*, Beverly Hills Concepts, Inc. v. Schatz & Schatz, 717 A.2d 724, 730 (Conn. 1998) (pointing out that professionals' fiduciary obligations include more than simply exercising due care in delivering professional services, because professionals also owe a duty of loyalty to their clients); Caroline Forell & Anna Sortun, *The Tort of Betrayal of Trust*, 42 U. MICH. J.L. REFORM 557, 565-66 (2009) (arguing that although "[p]rofessional malpractice is . . . a kind of breach of fiduciary duty," the law should recognize a

context of contractual relationships, but the duty at stake is a tort duty — a failure to take appropriate care toward the patient or client, or a failure to act in the interests of the patient or client.[106]

Although professional malpractice and professional breach of duty normally arise out of a contract, courts regularly enforce tort duties that do not have to be spelled out in a contract or explicitly agreed to by the parties; they also award tort damages.[107] That is also true with respect to duties about information. Even absent an express promise not to reveal, use, or sell information, there is a duty not to do so in

separate cause of action for betrayal of trust); Dayna Bowen Matthew, *Implementing American Health Care Reform: The Fiduciary Imperative*, 59 BUFF. L. REV. 715, 732-34 (2011) (distinguishing duty not to act negligently from duty of loyalty).

On the other hand, some courts have held that suing a doctor for breach of fiduciary duty is simply duplicative of a malpractice claim because fiduciary obligations are already part of professional obligations. *See* Neade *ex rel.* Neade v. Portes, 739 N.E.2d 496, 503 (Ill. 2000); RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 49 cmt. c (2000) ("Many claims brought by clients against lawyers can reasonably be classified either as for breach of fiduciary-duty or for negligence without any difference in result."); Forell & Sortun, *supra*, at 565 n.34.

Still other courts treat malpractice as a catch-all term for separate causes of action. *See, e.g.*, Smith v. Mehaffy, 30 P.3d 727, 733 (Colo. App. 2000) ("Legal malpractice is a generic term for at least three distinct causes of action available to clients who suffer damages because of their lawyers' misbehavior. . . . (1) [B]reach of contract, (2) breach of fiduciary duty, or (3) negligence.").

106 *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 49 (2000) ("[A] lawyer is civilly liable to a client if the lawyer breaches a fiduciary duty to the client."); *id.* § 53 cmt. g; RESTATEMENT (SECOND) OF TORTS § 299A cmt. b (1965) (explaining that tort duty to exercise reasonable care "applies to any person who undertakes to render services to another in the practice of a profession, such as that of physician or surgeon, dentist, pharmacist, oculist, attorney, accountant, or engineer"); *see also* Ray Ryden Anderson & Walter W. Steele, Jr., *Fiduciary Duty, Tort and Contract: A Primer on the Legal Malpractice Puzzle*, 47 SMU L. Rev. 235, 241-42 (1994) (noting that although fiduciary relationships may arise in contract, the law enforces them through stricter fiduciary standards); *id.* at 245-46 (explaining that the law of malpractice and other fiduciary obligations add tort-like duties to relationships that begin as contracts); *cf.* TAMAR FRANKEL, FIDUCIARY LAW 240-41 (2011) (arguing that fiduciary duties should be understood as distinct from ordinary tort obligations but that they have important similarities, including non-waivable duties and remedies that go beyond contract damages).

107 *See* RESTATEMENT (SECOND) OF TORTS § 874 & cmt. b (1979) (explaining that "[a] fiduciary who commits a breach of his duty as a fiduciary is guilty of tortious conduct to the person for whom he should act" and is subject to tort damages in addition to restitutionary or other remedies); sources cited *supra* note 106; *cf.* Daniel Markovits, *Sharing Ex Ante and Sharing Ex Post: The Non-Contractual Basis of Fiduciary Relations*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 209, 209-10 (Andrew S. Gold & Paul B. Miller eds., 2014) (noting that, unlike in contract, the law rejects the notion of efficient breach of fiduciary duties, and permits the award of punitive damages).

ways that will harm the interests of the client or that pose a conflict of interest between the professional and the patient or client.[108]

Why do the parties not have to spell out their obligations through contract in these relationships? The implied contract theory does not really answer this question; it simply asserts that there are implied terms that emerge from unstated or customary obligations. But where do these obligations come from in the first place? Equally important, why do they sometimes allow recovery of tort damages rather than more limited contractual damages? The answer is that doctors, lawyers, and accountants have special relationships of trust and confidence with their clients. These are fiduciary relationships.[109]

Generally speaking, a fiduciary is one who has special obligations of loyalty and trustworthiness toward another person. The fiduciary must take care to act in the interests of the other person, who is sometimes called the principal, the beneficiary, or the client. The client puts their trust or confidence in the fiduciary, and the fiduciary has a duty not to betray that trust or confidence.[110]

Fiduciaries often perform professional services or else manage money or property for their principals, beneficiaries, or clients. In almost every case, however, fiduciaries also handle sensitive personal information. That is because, at their core, fiduciary relationships are relationships of trust and confidence that involve the use and exchange of information.

Fiduciaries have two basic duties. The first is a duty of care. The fiduciary must take care to act competently and diligently so as not to

---

[108] *See, e.g.*, MARK A. HALL, MARY ANNE BOBINSKI & DAVID ORENTLICHER, MEDICAL LIABILITY AND TREATMENT RELATIONSHIPS 171 (3d ed. 2013) (collecting cases on duties of patient confidentiality); *see also* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS §§ 16, 49, 60 (2000) (stating lawyers' fiduciary duties to respect client confidences and to act in the client's interests); Janet Leach Richards & Sheryl Wolf, *Medical Confidentiality and Disclosure of Paternity*, 48 S.D. L. REV. 409, 413 & n.20 (2003) (collecting cases which hold that "that a patient can recover damages for a breach of a physician's duty of confidentiality").

[109] *See* FRANKEL, *supra* note 106, at 42-45; *see also* RESTATEMENT (SECOND) OF TORTS § 874 reporter's note (1979) ("One breach of fiduciary duty that is more commonly regarded as giving rise to an action in tort is the disclosure of confidential information." (citations omitted)).

[110] *See, e.g.*, Kurtz v. Solomon, 656 N.E.2d 184, 190 (Ill. App. Ct. 1995) ("A fiduciary relationship exists when one person places trust and confidence in another who, as a result, gains influence and superiority over the other."); Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 882 (explaining that fiduciaries "must be loyal to the interests of the other person" and that "the fiduciary's duties go beyond mere fairness and honesty; they oblige him to act to further the beneficiary's best interests").

harm the interests of the principal, beneficiary, or client.[111] The second, and in many ways more important duty, is the duty of loyalty. Fiduciaries must keep their clients' interests in mind and act in their clients' interests.[112] As a result, fiduciaries also have a duty not to create potential or actual conflicts of interest that might undermine their duties of loyalty and lead them to undermine the interests of their clients.[113]

Relationships of trust and confidence are often centrally concerned with the collection, analysis, use, and disclosure of information.[114] Lawyers and doctors, who act under a duty of confidentiality, often obtain information that would be very embarrassing to their clients or might be used to their disadvantage. So, in general, the duties of a fiduciary include duties not to use information obtained in the course of the relationship in ways that harm or undermine the principal, patient, or client, or create conflicts of interest with the principal, patient, or client.[115]

Put differently, professionals like doctors and lawyers have fiduciary obligations that give them special duties with respect to personal information that they obtain in the course of their relationships with their clients. Therefore, we can give them a special name. We can call them *information fiduciaries*.

---

[111] FRANKEL, *supra* note 106, at 169-72; *see also* RESTATEMENT (THIRD) OF AGENCY § 8.08 (2006) ("[A]n agent has a duty to the principal to act with the care, competence, and diligence normally exercised by agents in similar circumstances."); *see also* RESTATEMENT (SECOND) OF TORTS § 299A & cmt. b (1965) (describing tort duty to exercise the customary care of persons in a given profession).

[112] FRANKEL, *supra* note 106, at 4, 106-08; *see also* RESTATEMENT (THIRD) OF AGENCY § 8.01 (2006) ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship."); *see also* Deborah A. DeMott, *Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences*, 48 ARIZ. L. REV. 925, 936-37 (2006) (arguing that a justified expectation of loyalty is the characteristic feature of all fiduciary relationships).

[113] FRANKEL, *supra* note 106, at 108.

[114] *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1308-10 (2000) (arguing for basing privacy law on breach of trust); Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, STAN. TECH. L. REV. (forthcoming) (manuscript at 6-7), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2655719 (arguing that privacy law should be grounded in concepts of trust in the use of information similar to fiduciary law).

[115] *See* RESTATEMENT (THIRD) OF AGENCY § 8.05 (2006) ("An agent has a duty . . . (2) not to use or communicate confidential information of the principal for the agent's own purposes or those of a third party."); *see also* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS §§ 16, 49, 60 (2000) (stating lawyers' fiduciary duties to respect client confidences); HALL, BOBINSKI & ORENTLICHER, *supra* note 108, at 171 (stating fiduciary duties of physicians).

An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship.[116] People and organizations that have fiduciary duties arising from the use and exchange of information are information fiduciaries whether or not they also do other things on the client's behalf, like manage an estate or perform legal or medical services. Because most professional relationships are fiduciary relationships, most professionals are also information fiduciaries. And that means, in particular, that professionals have duties to use the information they obtain about their clients for the client's benefit and not to use the information to the client's disadvantage.

Fiduciary duties are, generally speaking, duties of trust. In fact, the term "fiduciary" comes from the Latin word for "trust;" and there is a similar connection between the words "confidentiality" and "confidence," or trust in another.[117] In fact, the idea of an information fiduciary is related to the law of confidentiality. Neil Richards and Dan Solove have argued that we should expand the common law of confidentiality, which recognizes a tort for breach of confidentiality when a person violates a relationship of trust with another.[118] The proposed Restatement of Data Privacy Principles recognizes a duty to maintain confidentiality where there is an "express or implied promise of confidentiality" or in light of relevant "ethical standards."[119]

IV. FIDUCIARIES AND THE FIRST AMENDMENT

How does the idea of an information fiduciary interact with the First Amendment? Does being an information fiduciary affect one's free speech rights? Yes, it does. The First Amendment treats information practices by fiduciaries very differently than it treats information practices involving relative strangers.

Suppose that you are a gynecologist, and in the course of your practice, you learn all sorts of interesting things about your patients, including the crazy things your patients say to you. You decide to comment on what you have learned by making a work of art,

116 Balkin, *Information Fiduciaries*, *supra* note 4.

117 *See also Fiduciary*, BLACK'S LAW DICTIONARY (10th ed. 2014); ADOLF BERGER, ENCYCLOPEDIC DICTIONARY OF ROMAN LAW 471-72 (1953).

118 Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 156-58, 182 (2007); *see also* Litman, *supra* note 114, at 1308-10 (arguing for breach of trust and breach of confidence as the basis of information privacy law); Richards & Hartzog, *supra* note 114.

119 RESTATEMENT OF DATA PRIVACY PRINCIPLES § 5 (Preliminary Draft No. 2, 2014).

appropriately entitled, "Crazy Stuff My Patients Say." You create an art installation at a contemporary art museum. It features a rotating cylinder with flashing lights on which are projected pictures of your patients, and quotes of interesting things that patients have said to you in the course of your practice; surrounding the cylinder, encased in plastic, are copies of case histories and medical reports. You present this to the public as a work of art that offers a profound commentary on the state of medicine and the nature of the human body in the twenty-first century.

Your patients are understandably annoyed to see themselves featured in your art, and they sue you for malpractice or for breach of a professional (fiduciary) duty. You defend yourself on the grounds that you are an artist, and you point out that your work, like the best contemporary art, is designed to be transgressive. Yet the fact that you are an artist, who makes amazing works of art with your patients' personal data and medical records, would probably not be a sufficient defense in a tort action for malpractice or breach of professional duty.[120]

Why is this? Well, you are using sensitive information to your advantage and to the disadvantage of your patients. Generally speaking, when the law prevents a fiduciary from disclosing or selling information about a client — or using information to a client's disadvantage — this does not violate the First Amendment, even though the activity would be protected if there were no fiduciary relationship.

To explain why this is so, I will borrow an idea from my friend and colleague, Dean Robert Post. Post points out that our First Amendment jurisprudence gives special protection to what he calls *public discourse*.[121] Public discourse refers to the processes of communication through which ideas and opinions circulate in a community to produce public opinion.[122]

---

[120] *See, e.g.*, Doe v. Roe, 400 N.Y.S.2d 668 (Sup. Ct. 1977) (holding a psychiatrist liable for breach of duty of confidentiality for republishing parts of a patient's analysis in a book); *see also* Horne v. Patton, 287 So. 2d 824, 829-30 (Ala. 1973) (recognizing physician's duty not to disclose information obtained in course of patient's treatment); Cannell v. Med. & Surgical Clinic, 315 N.E.2d 278, 280 (Ill. App. Ct. 1974) (same); McCormick v. England, 494 S.E.2d 431, 439 (S.C. Ct. App. 1997) (same).

[121] Robert C. Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 601, 637-38 (1990) (defining public discourse as "critical interaction" between members of a community and noting that "[c]ontemporary constitutional doctrine looks to this debate to constitute that 'universe of discourse' within which public opinion, and hence democratic policy, may be formed").

[122] *See, e.g.*, ROBERT C. POST, CITIZENS DIVIDED: CAMPAIGN FINANCE REFORM AND THE

Post and I have slightly different views about why public discourse receives special constitutional protection. He argues that the Constitution protects public discourse because it promotes democratic legitimacy. For government to be responsive to its citizens, it must respect the free circulation of ideas and opinions.[123]

I agree that this is one reason why we value public discourse, but it is not the only one. Most of what people discuss in public discourse is not especially political. They discuss celebrities, sports, popular entertainment, art, and music, and they talk about their relationships with others and their personal lives. These discussions are very important to people; more important, in some cases, than their views on electoral politics or public policy. People are social creatures, and they become who they are through conversation, through absorbing popular art and culture, and through being influenced by the ideas and opinions of the people around them.

People influence and reshape each other over time by living and participating in cultures of belief and opinion, and so these cultures have significant power over people. Cultures often feature powerful institutions and practices that produce and reproduce beliefs and opinions. People have a right to participate in forms of power that reshape and alter them because what is literally at stake is their own selves. The central way that people participate in the formation of cultures of belief and opinion is through freedom of expression (including associated freedoms like those of press, assembly, and association).

In a free society, even in one that is not perfectly democratic, or even democratic at all, people should have the right to participate in the forms of meaning-making that shape who they are and that also help constitute them as individuals, whether or not their speech has much of a connection to politics.[124] For this reason, I argue that the

---

CONSTITUTION 49 (2014) [hereinafter CITIZENS DIVIDED] ("I shall use the term *public discourse* to describe the communicative processes by which persons participate in the formation of public opinion."); ROBERT C. POST, DEMOCRACY, EXPERTISE, AND ACADEMIC FREEDOM: A FIRST AMENDMENT JURISPRUDENCE FOR THE MODERN STATE 15 (2012) [hereinafter DEMOCRACY, EXPERTISE, AND ACADEMIC FREEDOM] (same).

123 POST, CITIZENS DIVIDED, *supra* note 122, at 49-50 (explaining that the First Amendment's protection of the right of participation in public discourse underwrites citizens' belief that their government is responsive to them); Robert Post, *The Constitutional Status of Commercial Speech*, 48 UCLA L. REV. 1, 7 (2000) ("Public discourse is comprised of those processes of communication that must remain open to the participation of citizens if democratic legitimacy is to be maintained.").

124 Jack M. Balkin, *Cultural Democracy and the First Amendment*, 110 NW. U. L. REV. (forthcoming 2016) (manuscript at 10), *available at* http://papers.ssrn.com/sol3/

First Amendment protects the right to participate in the formation of culture as well as in political discourse. The First Amendment, in other words, protects *cultural democracy* as well as *political democracy*.[125] Indeed, political democracy is made possible by the institutions of cultural democracy.

Meaning-making through cultural participation and comment, as well as mutual influence through the circulation of opinions, long predated the rise of modern democracies, and so its value is not limited to supporting democratic legitimacy. Moreover, in the digital age, cultural participation is not limited to national boundaries, and in fact, it does not respect national boundaries. So the right to participate in culture has an importance and a value that transcends legitimating political power within a single state. To be sure, Post is correct that the right to participate in culture through public discourse is necessary to produce the kind of public opinion that could legitimate a democratic state, but this right has independent constitutional value. Thus, the right of freedom of expression is not only the right to participate in democracy, but also the right to participate in a *democratic culture*.[126]

The differences between Post's formulation and mine do not matter significantly for purposes of this essay. Under either account, what the First Amendment principally protects is our ability to participate in the formation of public opinion through expressing our ideas, beliefs, and opinions to each other. Freedom of speech gives human beings the right to have a say in the forms of cultural power that shape them and the forms of state power that govern them.

Under either account, many kinds of speech acts are not part of public discourse. They are not attempts to participate in the formation of public opinion by exchanging ideas, beliefs, and opinions. Instead, they are forms of market behavior that use speech. Therefore, states may regulate the speech involved in them.[127] For example, people use speech to form contracts (or to refuse to form contracts). In doing so, they are not engaged in public discourse, even though the speech occurs in public.

papers.cfm?abstract_id=2676027; *see* Balkin, *Digital Speech and Democratic Culture*, *supra* note 2, at 3-4, 35-37.

125 Balkin, *Cultural Democracy and the First Amendment*, *supra* note 124, at 9-10; Balkin, *Digital Speech and Democratic Culture*, *supra* note 2, at 3-4, 35-37.

126 Balkin, *Cultural Democracy and the First Amendment*, *supra* note 124, at 10; Balkin, *Digital Speech and Democratic Culture*, *supra* note 2, at 3-4, 35-37.

127 Robert Post & Amanda Shanor, *Adam Smith's First Amendment*, 128 HARV. L. REV. F. 165, 179 (2015), *available at* http://harvardlawreview.org/2015/03/adam-smiths-first-amendment/.

Hence, the state can regulate what people say to each other as they form (or refuse to form) contracts, as it does in antitrust law, consumer protection law, and antidiscrimination law. For the same reason, government can regulate the warnings and information that companies put on product labels that are read by members of the general public. And financial prospectuses for publicly traded companies are not part of public discourse, even though the companies are publicly traded.[128] Therefore, without falling afoul of the First Amendment, governments can regulate contracts to prevent discrimination and unfair business practices; they can require companies to label their products and make disclosures to protect consumers; and they can require companies to disclose information about themselves and about their operations in order to protect investors.

Commercial speech is a special case. Like contractual speech, it is a form of market behavior. Its social function is to induce people to buy goods and services. But unlike the speech involved in bargaining over contracts, commercial speech actively tries to reshape popular culture in order to sell products and services. It does so by providing information, ideas, images, and opinions to the general public, attempting to reshape people's self-image, beliefs and desires.[129] Commercial speech, in other words, is market behavior that attempts to alter public culture to facilitate itself. The hybrid nature of commercial speech — as affecting public opinion but not participating in public discourse — shapes the distinctive way that the First Amendment treats it.

Constitutional doctrine does not treat advertisers as attempting to participate in public discourse. Rather, it views advertisers as adding information that might be valuable to people who are participating in public discourse. As the Court explained in *Central Hudson*, "[t]he First Amendment's concern for commercial speech is based on the informational function of advertising."[130] Thus, the First Amendment focuses not on the right of the advertiser to speak but on the right of the public to receive the advertiser's information.[131]

---

[128] *See* Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1777-84 (2004) (noting large swaths of business regulation, including labor law, antitrust law and securities regulation, that remain largely outside the coverage of the First Amendment).

[129] *See* Balkin, *Cultural Democracy and the First Amendment*, *supra* note 124, at 50-51.

[130] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 563 (1980) (citing First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 783 (1978)).

[131] Post & Shanor, *Adam Smith's First Amendment*, *supra* note 127, at 172 (noting that the Supreme Court "explicitly created commercial speech doctrine to protect the rights of *listeners* rather than the autonomy of *speakers*"); Post, *The Constitutional*

If the First Amendment treated advertisers as contributing to public discourse, courts would protect the right of advertisers to speak in the same way that they protect politicians who shade the truth or mislead their audiences.[132] But because the First Amendment focuses on the right of the public to receive information, the rules are quite different. Advertising information is valuable to the public to the extent that it is true (or at least not misleading). Therefore, governments must protect truthful, non-misleading commercial speech; but, at the same time, governments may also require advertisers to alter or supplement their advertisements to inform consumers or to avoid misleading them.[133]

As the examples of contractual and commercial speech demonstrate, what falls within public discourse and what falls outside of it does not depend on the content of the speech. Rather, it depends on a characterization of social relationships. It depends on our understanding of social function and on what people are doing when they communicate with each other. In First Amendment law, deciding whether regulation of communication is content-neutral or content-based is often less important than deciding how to characterize the social relationships in which communication occurs.[134]

When people engage in public discourse, either as speakers or as audiences, the law presumes that they are free, independent, and autonomous, even if they are really not.[135] Hence, it does not allow

Status of Commercial Speech, *supra* note 123, at 14-15 (noting that the Supreme Court's analysis has been "audience oriented").

132 *Cf.* United States v. Alvarez, 132 S. Ct. 2537 (2012) (applying strict scrutiny to strike down federal law that criminalized falsely claiming to have been awarded military honors).

133 *See* Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651 (1985) ("Because the extension of First Amendment protection to commercial speech is justified principally by the value to consumers of the information such speech provides, appellant's constitutionally protected interest in *not* providing any particular factual information in his advertising is minimal." (citation omitted)).

134 Moreover, it also matters how *the state* characterizes speech. If the state treats and regulates market behavior as public discourse, courts should apply the traditional rules that apply to public discourse. Thus, if governments treated commercial advertisements differently because of their political message, courts should apply strict scrutiny. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 388-89 (1992) ("[A] State may not prohibit only that commercial advertising that depicts men in a demeaning fashion.").

135 "False ideas," Robert Post explains, "are not constitutionally recognized as causing harm within public discourse because persons within that discourse are presumed to be autonomous and independent." Robert C. Post, Response, *Reply to Bender*, 29 ARIZ. ST. L.J. 495, 499 (1997). On the other hand, "false ideas are deemed capable of causing compensable harms within doctor-patient relationships because

paternalistic restrictions on the dissemination of ideas and opinions, even though it is entirely predictable that some people, perhaps many, will be deceived or confused. All persons (or at the very least, all adults) are treated as equally competent and equally able to fend for themselves in the realm of public discourse. Therefore, even if speech misleads or harms people, the First Amendment normally protects it.[136]

But when people engage in speech that is not characterized as part of public discourse, the First Amendment treats their behavior quite differently. Outside of the realm of public discourse, the law drops its assumption that everyone is equally able, independent, and knowledgeable, and that everyone can equally fend for themselves.[137]

This is another way of seeing why advertisers are not participating in public discourse, even though they are surely trying to shape public opinion. The First Amendment allows governments to assume that consumers may not be able to assess market risks without compelled disclosures and prohibitions on misleading advertisements.

This distinction is especially important in the context of economic and professional transactions. The law often treats people as potentially uninformed, vulnerable, and dependent in many economic and professional relationships, even when these relationships involve speech. In fact, many economic and professional transactions not only involve speech, they would be impossible without speech. Imagine a stock market where no one could communicate prices or a hospital where doctors and patients could say nothing to each other. Friedrich Hayek's famous defense of markets is that they are dispersed social arrangements for exchanging information.[138] The idea of economic activity depends on the circulation, use, and communication of information. But economic activity is not public discourse in the First

persons in that context are presumed to be trusting and dependent." *Id.*

136 *See, e.g.*, Snyder v. Phelps, 562 U.S. 443, 461 (2011) ("As a Nation we have chosen a different course — to protect even hurtful speech on public issues to ensure that we do not stifle public debate.").

137 POST, DEMOCRACY, EXPERTISE, AND ACADEMIC FREEDOM, *supra* note 122, at 23 ("Whereas within public discourse the political imperatives of democracy require that persons be regarded as equal and as autonomous, outside public discourse the law commonly regards persons as dependent, vulnerable, and hence unequal.").

138 F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 526 (1945) ("[I]n a system where the knowledge of the relevant facts is dispersed among many people, prices can act to coördinate the separate actions of different people in the same way as subjective values help the individual to coördinate the parts of his plan.").

Amendment sense. Otherwise, all economic transactions involving speech would be constitutionally protected.[139]

For the same reason, the speech that occurs in fiduciary relationships is not public discourse. When law regulates professional relationships with clients in fields like law or medicine, it often regulates the way that professionals speak to clients and requires that they not use client information against the client's interest.[140] The law characterizes the social function of speech in these relationships as importantly different from the expression and circulation of opinions in the public sphere. In fiduciary relationships, the fiduciary communicates with a person who seeks special services (often professional services) and who is made vulnerable and dependent on another because of the need for those services.

Tort and fiduciary law assume that professionals and their clients do not stand on an equal footing. Professionals have special skill and knowledge that clients often lack. Clients are usually dependent on professionals to perform important tasks for them. They cannot easily specify how professionals should perform these tasks because they lack the appropriate skills. Clients usually are ill-prepared to monitor the behavior of professionals and to prevent them from abusing relationships of trust. Because of the asymmetry of skill and understanding between professionals and their clients, and because clients are not very good at monitoring professional conduct, clients must put themselves in the hands of professionals and trust them to act in the client's best interest.[141] And given the information that

---

[139] *Cf.* Post & Shanor, *Adam Smith's First Amendment*, *supra* note 127, at 171-72 (noting that expanding the definition of speech to include a wide range of economic activity would drastically shrink the space of democratic lawmaking).

[140] *See supra* notes 105–19 and accompanying text.

[141] *See* FRANKEL, *supra* note 106, at xvi, 4, 6, 18, 29 (noting that these asymmetries are characteristic of most of fiduciary relationships). Thus, many scholars have derived fiduciary obligations from contract as well as from tort principles. Contractual theories of fiduciary obligation generally argue that fiduciary duties occur in exceptional situations because of the nature of the bargaining relationship between the parties. Courts, in essence, impose the kinds of terms that the parties would have adopted if there were not significant informational and monitoring costs. Thus, Easterbrook and Fischel argue, "[A] 'fiduciary' relation is a contractual one characterized by unusually high costs of specification and monitoring. The duty of loyalty replaces detailed contractual terms . . . ." Frank H. Easterbrook & Daniel R. Fischel, *Contract and Fiduciary Duty*, 36 J.L. & ECON. 425, 426-27 (1993); *see also* John H. Langbein, *The Contractarian Basis of the Law of Trusts*, 105 YALE L.J. 625, 657-58 (1995) (arguing that similar considerations apply to trust law, which is essentially contractual). Roberta Romano has pointed out that asymmetry of information between the parties is often an important feature of fiduciary relationships and that many

clients must give professionals, clients' relative lack of knowledge, and clients' inability to monitor professional behavior and assess risk, it is especially easy for professionals to abuse that trust. This is the opposite of the model of independent, autonomous individuals presupposed by the model of public discourse.

For these reasons, the law does not treat speech in professional or other fiduciary relationships as part of public discourse; instead, it treats speech within these relationships as part of ordinary social and economic activity that is subject to reasonable regulation. The concept of public discourse creates a distinction between what is "public" and what is not "public," but it is not the distinction between what is widely known and what is secret. Rather, it is a distinction between what kind of speech is connected to the constitutional values behind the First Amendment — the circulation of ideas and opinions among the public — and what kind of communication serves other values and social functions and is therefore properly subject to democratic regulation.

A good example of how the law characterizes social relations as falling inside or outside of public discourse is *Lowe v. SEC*.[142] *Lowe* upheld the right of people who are not registered as investment advisors to publish newsletters offering advice about securities to the general public.[143] Interpreting the Investment Advisers Act of 1940, the Court distinguished between people who offer advice to the general public and people who offer advice to particular people about what securities to purchase or sell.[144] This distinction tracks the distinction between public discourse and other kinds of speech. When people offer advice to the general public, they are not engaged in individualized advice to clients. They speak to anyone who will listen, and so we say that they are engaged in public discourse. But when

monitoring problems may be due to information asymmetry. Roberta Romano, Comment, *Comment on Easterbrook and Fischel, "Contract and Fiduciary Duty*," 36 J.L. & ECON. 447, 448 (1993).

Romano also points out that a purely contractual approach to fiduciary duty may not be able to explain a wide range of fiduciary duties that are imposed by statute, and which do not allow the same degree of flexibility as common-law contract. *Id.* at 449. Similarly, Daniel Markovits has pointed out that the fact that fiduciaries enter into relationships through contract does not mean that their duties are defined by contract. Many fiduciary relationships limit the ability of parties to modify terms and impose duties beyond contract. Markovits, *supra* note 107, at 209-10, 221 (using the example of marriage).

142 472 U.S. 181 (1985).

143 *Id.* at 211.

144 *Id.* at 210-11.

advisors work with individual clients, the social context is different. They are not announcing their views to the general public. Instead, they purport to perform professional services for individual customers. Therefore Congress may, if it wishes, require them to register as investment advisors and assume certain duties.[145]

Note that the Court did not say that Congress *must* treat investment advisors as fiduciaries, much less treat them like doctors or lawyers. Instead, the Court simply assumed that, consistent with the First Amendment, Congress *may* treat investment advisors as fiduciaries or impose some fiduciary-like obligations on them.[146] Because these investment advisors are not engaged in public discourse, the First Amendment does not preempt Congress's choice. Congress may reasonably conclude that investment advisors perform services that require a certain degree of trust and confidence between themselves and their clients. But it may also conclude that regulation would be unwise. Once we characterize speech as falling outside of public discourse, there is still the further question of what kinds of regulation are most appropriate.[147]

---

[145] *Id.* at 210. The Court noted that Congress was "plainly sensitive to First Amendment concerns" in adopting the Investment Advisers Act, and "wanted to make clear that it did not seek to regulate the press through the licensing of nonpersonalized publishing activities." *Id.* at 204. Hence, while deciding the case on statutory grounds, the Court invoked First Amendment principles because Congress "was undoubtedly aware" of the Court's First Amendment jurisprudence prior to the Act. *See id.* at 204-05 (citing Lovell v. City of Griffin, 303 U.S. 444 (1938); Near v. Minn. *ex rel.* Olson, 283 U.S. 697 (1931)). Moreover, in determining that the relevant publications fell within the statutory exclusions to registration under the Act, the Court noted their factual and general nature and that they were undoubtedly protected under the First Amendment. *Id.* at 210 & n.58.

[146] *Id.* at 210.

[147] To be sure, there may be First Amendment rights within professional relationships, but they are based on different kinds of concerns than the protection of public discourse. For example, in order to fulfill their social function as learned professionals, doctors must be able to provide truthful information to their patients. This is a First Amendment right, but it is not a right to engage in public discourse — after all, it is directed at a patient in a confidential relationship. Rather it stems from other constitutional values underlying the First Amendment — in particular, a constitutional interest in the development and faithful application of professional knowledge. Thus, if the state required doctors to lie to their patients about treatment options, or required doctors to parrot junk science, there might be a First Amendment problem, notwithstanding the state's general authority to regulate medical care. *See, e.g.*, Robert Post, *Informed Consent to Abortion: A First Amendment Analysis of Compelled Physician Speech*, 2007 U. ILL. L. REV. 939, 986, 989-90 (arguing that the right to integrity of physician patient relationships is partially protected by the First Amendment); Claudia E. Haupt, *Professional Speech*, 125 Yale L.J. 1238 (2016) (arguing that the First Amendment protects the ability to express professional

In *Lowe* itself, the Court suggested that ordinary First Amendment doctrine — including even the ban on prior restraints — would not apply to communications between investment advisors and their clients.[148] In the Court's words, personalized communications create special dangers of "fraud, deception, or overreaching" that "are not replicated in publications that are advertised and sold in an open market."[149] The Court is not asserting that people do not engage in false or misleading claims in public discourse — they do so all the time. Rather, the Court's point is that these speakers are not engaged in the sort of personalized advice in which fraud, deception and overreaching create special dangers for vulnerable clients. The Court therefore distinguished between "impersonal" communications between newspapers and subscribers and "the kind of fiduciary, person-to-person relationships . . . that are characteristic of investment adviser-client relationships."[150]

Information about clients that is obtained in the course of fiduciary relationships is not public discourse. Therefore, when a fiduciary communicates private information about a client to the public, the communication does not receive standard First Amendment protection, unless the dependent person — the client — permits the information to enter public discourse.

This explains why, in my hypothetical, the art exhibit, "Crazy Stuff My Patients Say," does not receive full First Amendment protection even though it takes the form of contemporary art. It uses information obtained in a fiduciary relationship without permission from the affected patients. Similarly, suppose a lawyer or doctor becomes a presidential candidate and reveals embarrassing information about clients to bolster his or her electoral chances. Even though the content of the speech is political and its purpose is political, the speech is not immune from regulation, because it is an abuse of a confidential relationship in which the candidate was an information fiduciary. If this were not so, then any professional could get around malpractice law by claiming to be an artist or a politician.

It is important to note that these are special cases. Not everyone that I deal with is an information fiduciary with respect to me — most people are not. Suppose that a person illegally obtains my medical reports and presents them to a reporter. The reporter publishes them

opinions as well as the ability to participate in the production and development of professional knowledge).

148 *See Lowe*, 472 U.S. at 204.

149 *Id.* at 210.

150 *Id.*

because the reporter reasonably believes that the information in them is newsworthy. If the reporter did not obtain the information illegally, and if the information otherwise involves a matter of public concern, then, under *Bartnicki v. Vopper*, the reporter can publish the information without fear of sanction.[151]

The difference in this case is that the reporter and I do not have a fiduciary relationship. So what the reporter learns lawfully can be placed in public discourse. On the other hand, I can sue the doctor for failure to protect my sensitive data, and I can also sue the person who hacked into my data in the first place. Moreover, the doctor has a fiduciary duty to make sure that, absent my consent, the doctor does not disclose this information to anyone except persons and institutions that apply the same privacy principles that the doctor is bound by. In other words, the doctor has a fiduciary duty to ensure that the privacy protections run with the data. The requirement that privacy protections run with the data means that I do not have to have a separate contractual agreement with everyone who handles the data. Rather, it is the fiduciary's job to ensure that my privacy is protected.

The idea of information fiduciaries helps us understand the limitations of the free speech theories we considered earlier. It explains why the argument that "commodified data is not speech" is not the best approach to privacy regulation. The question is not the form the information takes but how it is obtained and how it is used in the context of relations of dependence and trust. Commodified data can easily be part of public discourse and fully protected, for example, as part of scientific communication, journalism, or art.

Similarly, we can now see why the attempt to treat collections of personal data as commercial speech is tempting but also wrong. Characterizing data as commercial speech implicitly recognizes that the data is somehow not fully public discourse and therefore should deserve less than full First Amendment protection. But the characterization misunderstands *why* the data falls outside of public discourse. It falls outside of public discourse because it is collected and used in the context of a special relationship with fiduciary duties. Generally speaking, you do not have a fiduciary relationship with advertisers in the media who try to get you to buy their products. But in certain circumstances, you might have a fiduciary relationship with online service providers, especially if you must trust and depend on them, and they, in turn, encourage your trust and dependence.

---

[151] *See* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) ("[A] stranger's illegal conduct [in obtaining the material] does not suffice to remove the First Amendment shield from speech about a matter of public concern.").

V. INFORMATION FIDUCIARIES IN THE DIGITAL AGE

The law of fiduciary relationships developed historically, and the law has recognized new relationships over time.[152] The digital age, I argue, has given rise to new fiduciary relationships created by the explosion of the collection and use of personal data. The relationships of trust between end-users and online service providers need not be identical to traditional professional relationships in all respects. Equally importantly, these relationships may not require the same degree of obligation, loyalty, and protection that applied to older forms of professional relationships.

I do not claim that Facebook or Uber is managing my estate, or is my accountant, my doctor, or my lawyer. What I do claim is that in the digital age, because we trust them with sensitive information, certain types of online service providers take on fiduciary responsibilities. These responsibilities are not identical to those of older kinds of fiduciaries but have similarities to them. "Just as we recognized in the past that certain professionals were fiduciaries of our information," Neil Richards has explained, "so, too, in the Age of Information should we expand our definition of information fiduciaries to include bookstores, search engines, ISPs, email providers, cloud storage services, providers of physical and streamed video, and websites and social networks when they deal in our intellectual data."[153]

Why should we recognize new classes of information fiduciaries in the digital age? And why should we call their relationships with end-users *fiduciary* relationships? We should do so for the same reason the law recognized older forms of fiduciary duties in the past.

---

[152] *See, e.g.*, Tamar Frankel, *Fiduciary Law*, 71 CAL. L. REV. 795, 795-96 (1983) (discussing the rise of new forms of fiduciary obligation in the eighteenth and twentieth centuries); David J. Seipp, *Trust and Fiduciary Duty in the Early Common Law*, 91 B.U. L. REV. 1011 (2011) (describing the development of fiduciary obligations in the English common law).

[153] NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 168 (2015). Jerry Kang and his colleagues have suggested the creation of a class of information fiduciaries who collect and store the personal information (e.g., locational information) that we generate about ourselves. Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 812, 831-32 (2012). Still earlier, Kenneth Laudon proposed creating a class of information fiduciaries who would manage our information assets for us. Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92, 101. *See generally* Richard R.W. Brooks, *Knowledge in Fiduciary Relations*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW, *supra* note 107, at 225, 240 (comparing the affirmative duties suggested by Laudon with the negative duties suggested by Richards).

First, end-users' relationships with many online service providers involve significant vulnerability, because online service providers have considerable expertise and knowledge and end-users usually do not. Online service providers have lots of information about us, and we have very little information about them or what they can do with the information they have collected. It is easy for online service providers to monitor what we do, especially as they collect increasing amounts (and kinds) of data about us. But it is generally very difficult for us to monitor their operations and prevent them from acting against our interests or otherwise betraying our trust.

Second, we find ourselves in a position of relative dependence with respect to these companies. They provide many different kinds of services that we need, and we must hope that they will not misuse our confidences or let loose information about us in ways that will harm us.

Third, in many cases, but not all, online service providers hold themselves out as experts in providing certain kinds of services in exchange for our personal information. For example, online dating services tell us they will match us with potential partners, online transportation services say they will match us with cars, search engines purport to give us the information we need quickly and efficiently, and so on.

Fourth, online service providers know that they hold valuable data that might be used to our disadvantage — and they know that we know it too. Therefore, they hold themselves out as trustworthy organizations who act consistent with our interests, even though they also hope to turn a profit.[154] They present themselves to the public as responsible and upstanding organizations who will use their power for lawful ends and, above all, who will not betray us.

Because people understand that they are vulnerable to the collection of personal data, and because they also recognize that the methods used by online service providers are beyond their understanding, they seek reassurance that using these services is safe. Online service providers are more than happy to offer those assurances, often in vague and general ways. The details are buried in the fine print of their privacy policies and in the code of the company's information infrastructure.[155] The details of these privacy policies may be

[154] *See, e.g.*, *Community Standards*, FACEBOOK, https://www.facebook.com/communitystandards (last visited Feb. 29, 2016) ("We want people to feel safe when using Facebook."); *Ten Things We Know To Be True*, GOOGLE.COM, https://www.google.com/about/company/philosophy/ (last visited Feb. 29, 2016) ("You can make money without doing evil.").

[155] *See, e.g.*, Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year*

technically available to the public, but their meaning and practical consequences may not be easy to understand, especially as companies come up with ever new uses and markets for information. And there is yet another kind of information asymmetry: the code of a company's information infrastructure and many of its operations are usually kept secret, often for entirely sensible reasons. Companies hope to preserve competitive advantage and to ward off security breaches.

By presenting themselves as trustworthy collectors and keepers of our individual data, and by emphasizing that, for reasons of security and competitiveness, they cannot be fully transparent, digital organizations induce relations of trust from us, so that we will continue to use their services.

I am not blaming companies for trying to make us feel safe in using their services. Quite the contrary. It is a good thing that companies attempt to induce trust and confidence, for much the same reason that it is good that doctors, lawyers, and accountants present themselves as reliable. In a complex society, people should be encouraged to use the services of learned professionals. In an even more complex information society, people should be encouraged to use the many new digital services that our world has to offer them. Just as a world without reliable professionals would be impoverished, a world without the business innovations of the digital age would also be impoverished.

For all of these reasons, we should recognize that a changing society generates new kinds of fiduciary relations and fiduciary obligations that the law can and should recognize. The scope of the fiduciary duty, however, is not the same for every entity. It depends on the nature of the relationship, the reasonableness of trust, and the importance of preventing self-dealing by the entity and harm to the end-user, client, or beneficiary.

Consider, then, a very basic — and necessarily vague — formulation: People and business entities act as information fiduciaries

> (1) when these people or entities hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them;
>
> (2) when these people or entities give individuals reason to believe that they will not disclose or misuse their personal information; and

Would Take 76 Work Days, ATLANTIC (Mar. 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ ("The collective weight of the web's data collection practices is so great that no one can maintain a responsible relationship with his or her own data.").

> (3) when the affected individuals reasonably believe that these people or entities 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.[156]

Note that this formulation may require information fiduciaries to protect more things than they have explicitly set out in their privacy policies. Obviously, organizations should be held accountable for violating their own privacy policies. But privacy policies may be intentionally vague, and they may not give fair warning of how the company will later use data. The proper question should be what forms of trust companies have induced in order to get people to use their services and what people may reasonably expect will be done with their data.

Perhaps the best way of summarizing the idea of information fiduciaries in the digital age is that online service providers may not act like con men. The term "con man" is short for "confidence man," and the point of a "con game" (or "confidence game") is to gain the trust and confidence of a mark in order to act against their interests later on.[157] The idea of a con game is just the mirror image of the idea of a fiduciary duty: if you induce another to treat you with confidence, you cannot turn around and betray that confidence.

Online service providers act like con men when they assure people that they will treat them fairly in order to obtain their business — and their data — and then betray them. In confidence games, betrayal may occur in wholly unexpected ways; indeed, if the mark saw the betrayal coming, they would not fall for it. We might make a similar point about the potential dangers of the digital world. Digital businesses are supposed to be creative; that is how they succeed. Yet, one side effect of being creative means that businesses will probably come up with ever new ways to use personal data, and therefore ever new ways to betray their end-users. The point of treating them as information fiduciaries is to encourage creativity without facilitating betrayal.

At a minimum, when entities hold themselves out as trustworthy, and when they encourage the disclosure of personal information that

---

[156] *See* RESTATEMENT OF DATA PRIVACY PRINCIPLES § 5.2 (Preliminary Draft No. 2, Oct. 24, 2014) (offering a similar test of confidentiality for "[r]elationships of trust").

[157] *See* M. ALLEN HENDERSON, FLIM-FLAM MAN: HOW CON GAMES WORK 3 (1985) ("As the term implies, the confidence artist gains the *confidence* of his victim in order to defraud him."); LIONEL S. LEWIS, CON GAME: BERNARD MADOFF AND HIS VICTIMS 2-3 (2012) ("What all con games have in common is that they attempt to victimize . . . by gaining the confidence of marks or victims.").

places end-users in a vulnerable position, entities should be held accountable for their representations. But the notion of information fiduciaries goes beyond explicit promises. Digital information fiduciaries may be held to reasonable ethical standards of trust and confidentiality, even if they do not make specific representations, because of the nature and kind of business they are in. In the same way, even if your doctor or lawyer does not explicitly promise confidentiality and good behavior, they are still information fiduciaries, and governments may impose legal obligations on them as such. It also follows that reasonable obligations placed on information fiduciaries do not violate the First Amendment, even if these regulations limit the ability to collect, analyze, use, sell, or disclose some kinds of end-user information.

These rules do not apply to everyone. Merely communicating with someone over the Internet does not make them an information fiduciary. That is why many collection, use, and disclosure practices will remain protected by the First Amendment.

VI. THE SCOPE OF FIDUCIARY OBLIGATIONS IN THE DIGITAL AGE

By suggesting that online service providers are information fiduciaries, I have been analogizing these companies to traditional professional fiduciaries like doctors or lawyers. This is analogy, however, and not an identity. Moreover, even within traditional examples, there is no single class of fiduciary duties that apply equally in all situations. The duties that courts impose depend on the nature of the relationships involved.[158] In the next part of this essay, I want to discuss important differences between the duties of digital information fiduciaries like Uber, Facebook, and Google, and traditional fiduciaries like doctors, lawyers, accountants, and managers of estates. The duties that we impose on traditional fiduciaries can be fairly extensive; but the duties we might justifiably impose on online service providers may be different and sometimes considerably narrower, especially if we want these duties to be consistent with the First Amendment.

Fiduciary duties or duties of confidentiality for doctors and lawyers are often quite broad and strong; they may be greater than we would

158 *See* FRANKEL, *supra* note 106, at 53 (noting that "[t]he process of recognizing new fiduciary relationships is ongoing," depending on the nature of their services, the power relations and temptations they create, and the ability of institutions and markets to control them); Frankel, *supra* note 152, at 810 ("Fiduciary relations vary by the extent to which each type of fiduciary can abuse his power to the detriment of the entrustor.").

reasonably expect of online service providers and related digital enterprises. We normally expect that doctors and lawyers will not say anything that harms their clients or creates a conflict of interest, and we expect these professionals to look out for our interests in many different ways. But people do not expect the same degree of concern from online service providers. Treating them as information fiduciaries is designed to keep these companies from harming end-users in a more limited set of ways.

There are good reasons for this. In most cases, people reward fiduciaries financially for the additional duties they take on. It is also important to organize payment so that it does not create a conflict of interest with the client; otherwise, the fiduciary's loyalties are divided between the client and the entity or organization providing funding. In the health care context, the institution of insurance perpetually raises this problem.

When we are dealing with online service providers like Facebook or Google, the most important source of compensation is personal information. For many online companies, the product or service is either free or heavily subsidized because it generates data, which is valuable to the company or to third parties to which the company sells the data.

All other things being equal, companies like Facebook or Google would like to maximize the value of the personal data they collect. And certainly if such a company goes bankrupt or is later sold, its collection of end-user data is one of its most valuable assets. The value of end-user data, and its centrality in the business models of many online service providers, creates an inherent potential for conflicts of interest between the digital company and the end-user.

We cannot rely on market forces alone to solve these conflict of interest problems. The market will work to some extent: markets may punish companies with bad reputations for mistreating their end-users. But there is no guarantee that this will be enough to effectively police all forms of misbehavior.

There are strong asymmetries of information between companies and end users. Online service providers' operations, algorithms, and collection practices are mostly kept secret — often for perfectly good reasons — because companies want to prevent free-riding from competitors and mischief from hackers. Even to the extent that companies' information practices are publicly available, end-users are not in a very good position to assess how well companies will protect their interests or to decide which company will treat them best in the long run. Nor can end-users easily predict how their data will be

collated, analyzed, and used in ways that affect their opportunities and interests. In many cases, end-users are largely dependent on the good will of these companies not to abuse their personal information.

Thus, online service providers present the familiar problems that generally give rise to fiduciary obligations. First, there are significant asymmetries of knowledge and information between online service providers and end-users. Second, it is very difficult for end-users to verify online companies' representations about data collection, security, use, and dissemination. Third, it is very difficult for end-users to understand what online companies do with their data and how data analysis and use affects their interests. Fourth, even if end-users understood these information practices, it would be almost impossible for end-users to monitor them.

All of these problems are connected to the inadequacy of relying on contract and property models to protect privacy and prevent overreaching. They are reasons for imposing some sort of fiduciary obligation on online service providers.

Nevertheless, if we impose fiduciary obligations that are too broad, it might follow that online service providers could not make any money at all from this data because the data might be used in some way to some end-user's disadvantage.

This is clearly too strong a claim. It cannot be the case that the basic business model of free or subsidized online services inherently violates fiduciary obligations and therefore can be made illegal. "Fiduciary" does not mean "not for profit." At the same time, consumers should be able to trust online service providers like Facebook, Uber, or Google not to abuse their ability to collect and use personal information for profit. An online business model should still be compatible with a range of fiduciary obligations.

It should be reasonable to expect that a transportation broker or an online dating service will not attempt or threaten to embarrass you to keep you from criticizing it. It is also reasonable to expect that a social networking service is designed to facilitate social networking and not to manipulate you into voting for the candidate of its choice because it wants to rig an election.

Because personal data is a key source of wealth in the digital economy, information fiduciaries should be able to monetize some uses of personal data, and our reasonable expectations of trust must factor that expectation into account. What information fiduciaries may not do is use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm.

We might make an analogy to financial advisors. We expect that financial advisors will make money from us when we ask them for advice about investments. We might allow a variety of different methods of compensation; advisors might be permitted to charge a small percentage of assets per year, or they might be permitted to charge us a small fee each time they ask for our advice. Even so, the fact that advisors make money from clients does not mean that we cannot impose any fiduciary obligations on them.[159] At the very least, governments should be able to require that investment advisors will be working for us and not for the mutual fund companies or financial institutions whose products they sell. Government may decide that financial advisors should not be beholden to other parties to avoid creating incentives to sell us products with hidden costs or high fees.

There is a second important difference between traditional fiduciaries and online service providers. Sometimes we expect that professionals will not only avoid actively harming clients but also look out for the interests of clients and keep them from harming themselves or doing foolish things.[160] Doctors, for example, present themselves as learned professionals concerned with our health; therefore, it is reasonable to expect them to warn patients about many kinds of health risks and not just to avoid incompetently treating the particular disease or condition that brings a patient to the doctor.

We might not want to impose comprehensive obligations of care on digital companies like Google, Facebook, or Uber. Their businesses are quite different from those of doctors, and they do not hold themselves out as taking care of end-users in general. The nature of their duties depends on the kind of business they present to the public. Google and Uber may have a duty to protect our privacy in certain ways, but we do not expect them to warn us not to go on a particular trip. Facebook presents itself as helping us to connect with other people. But we should not expect that Facebook has a fiduciary duty to warn us not to look up that long-lost college buddy who, it turns out, is a very dangerous person. Nor should we expect that Facebook has a

---

[159] For example, the Obama Administration has recently proposed new rules imposing fiduciary obligations on a larger class of investment advisors. JOHN J. TOPOLESKI & GARY SHORTER, CONG. RESEARCH SERV., R44207, DEP'T OF LABOR'S 2015 PROPOSED FIDUCIARY RULE: BACKGROUND AND ISSUES (2015), *available at* https://www.fas.org/sgp/crs/misc/R44207.pdf; *cf.* FRANKEL, *supra* note 106, at 45-47 (describing current debates over the fiduciary status of securities brokers).

[160] *Cf.* Richard R.W. Brooks, *Knowledge in Fiduciary Relations*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW, *supra* note 107, at 225, 240 ("Fiduciaries . . . have not only duties of confidentiality and disclosure, but also duties to inquire, to inform, [and] to speak with candor . . . .").

duty to keep us from receiving links from our Facebook friends that are misleading or emotionally disturbing. In these contexts, their duty to protect us is quite limited.

Third, digital companies like Facebook or Google may have an interest in getting people to express themselves as much as possible, thus creating links and content that can be indexed or shared with others. Social media companies may have an interest in getting people to disclose a lot about themselves. It is certainly possible that people may later regret how much they have disclosed. Although at some point that interest in promoting disclosure and production of content may create a conflict of interest between companies and end-users, we should not assume that online service providers have a positive obligation to stop asking people to reveal more of themselves in social media. Companies should have an obligation to facilitate end-users' control over their information and to explain the consequences of privacy settings, but not to prevent people from making every kind of bad choice in how they use social media.

We should think of these kinds of online service providers, in short, as special-purpose information fiduciaries. The nature of their services should guide our judgments about what kinds of duties it is reasonable to impose. We should connect the kinds of duties that information fiduciaries have to the kinds of services they provide. What is unexpected or seems like a breach of trust will depend on the kind of service that entities provide and what we would reasonably consider unexpected or abusive for them to do.

Because there are so many possible online services, including services nobody has yet imagined, legislatures and courts may find it difficult to draw lines initially. We might use tax breaks, safe harbors, legal immunities, or other incentives for organizations to accept fiduciary obligations rather than simply imposing them directly through government regulation. Therefore, as Jonathan Zittrain has suggested, it might be appropriate to offer online service providers an incentive to designate themselves as information fiduciaries in return for certain legal and financial benefits that come with the designation.[161]

Several years ago, Edward Castronova suggested that we might govern virtual worlds through what he called statutes of interration (a play on statutes of incorporation).[162] I adapted this idea in my own

[161] Jonathan Zittrain, *Facebook Could Decide an Election*, *supra* note 11.

[162] Edward Castronova, *The Right to Play*, 49 N.Y.L. SCH. L. REV. 185, 201-02 (2004).

work on virtual worlds.[163] I have argued that even though virtual environments are privately owned, governments could create framework statutes that would require platform owners to respect the free speech and privacy rights of end users in return for special legal status and benefits.[164] We might be able to adapt this idea to today's online service providers to create new classes of digital information fiduciaries.

VII. INFORMATION FIDUCIARIES AND THE FOURTH AMENDMENT

So far, I have discussed the relationship of information fiduciaries to the First Amendment. When I first wrote about the idea of information fiduciaries, however, I noted that it also might change the way we think about Fourth Amendment law.[165] As currently interpreted, the third-party doctrine holds that government does not have to obtain a warrant to obtain digital information about us that we have given to a third party.[166] This means that we have little or no Fourth Amendment protection when the government wants to obtain information collected about us that is in the hands of a social media site, ISP, or other online business. The law assumes that if we have consented to give this information to a third party, or have allowed a third party to collect it about us, we take the risk that the third party will disclose this information to the government. Therefore, we have no reasonable expectation of privacy in the information.[167]

The argument of this essay shows why that assumption is mistaken. We provide lots of information about ourselves — some of it quite sensitive — to people and organizations who owe us fiduciary duties or duties of confidentiality. And when we provide this information, we have, and should have, a reasonable expectation that they will respect our privacy. We have a reasonable expectation that disclosing this

---

[163] *See* Jack M. Balkin, *Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds*, 90 VA. L. REV. 2043, 2090-98 (2004) (arguing for framework statutes to protect free speech and privacy in certain kinds of multi-user online environments).

[164] *Id.* at 2092-95.

[165] *See* Balkin, *Information Fiduciaries*, *supra* note 4.

[166] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

[167] *See id.* at 588-90; *see, e.g.*, Smith v. Maryland, 442 U.S. 735, 743-45 (1979) (arguing that people have no reasonable expectation of privacy in the phone numbers they dial because they are available to phone companies; therefore "petitioner assumed the risk that the company would reveal to police the numbers he dialed"); United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." (citing United States v. White, 401 U.S. 745, 751-52 (1971))).

information to them, or allowing them to collect it from us, is not the same as making the information available to the public generally. We have a reasonable expectation, in other words, that people and organizations who owe duties of trust and confidence to us will not betray us. Indeed, the law creates and recognizes relationships of trust and confidence precisely because it wants people to have reasonable expectations of privacy in certain relationships.

If I am right that new digital online service providers may be new kinds of information fiduciaries, then we should have reasonable expectations of privacy in at least some of the information about ourselves that we share with them. The reasons why this information is not public discourse for purposes of the First Amendment also provide reasons why we should have a reasonable expectation of privacy for purposes of the Fourth Amendment.

This conclusion does not mean that the government may not obtain the information at all. The government may still use warrants upon a showing of probable cause. Or the information may fall under one of the exceptions to the warrant requirement.[168] The point, however, is that if we give information to an information fiduciary, the third-party doctrine should ordinarily not apply, and the information should not fall outside of the protections of the Fourth Amendment.

Note, moreover, that this would not be the end of the third-party doctrine. It would still continue to apply in all cases in which we provide information to someone who is not an information fiduciary. In fact, the concept of information fiduciaries is especially helpful because it gives us an intermediate position between enforcing the third-party doctrine as it currently stands and getting rid of it entirely.

Recently, Kiel Brennan-Marquez has taken up this project.[169] He points out that current Fourth Amendment doctrine often takes fiduciary-style relationships into account, although it does not map precisely onto the distinction between information fiduciaries and non-fiduciaries that I am drawing here.[170] Nevertheless, there is enough of an overlap that the doctrine could usefully move in this direction without too much disruption.

---

[168] *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 338 (2009) (exception to warrant requirement for search incident to lawful arrest); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989) (exceptions based on special needs).

[169] Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 611 (2015).

[170] *Id.* at 649-57.

VIII. INFORMATION FIDUCIARIES IN THE ALGORITHMIC SOCIETY

The theory of information fiduciaries does not solve all privacy problems. It does not deal with false light or the intentional infliction of emotional distress. It does not illuminate, much less solve, all problems of government invasion of privacy. Nevertheless, the theory of information fiduciaries allows us to understand how First Amendment guarantees of free speech can co-exist with regulatory solutions to a common set of problems created by the proliferation of data and uses of data in the digital age.

The key examples in my discussion so far have been online service providers — social media companies like Facebook, search engines like Google, and service platforms like Uber. But companies are increasingly using sophisticated algorithms and forms of artificial intelligence to make decisions about people in areas ranging from advertising to employment to policing to credit.[171] The Digital Society has become the Algorithmic Society.

The analysis I have just offered does not change if a company uses algorithms or artificial intelligence agents to harm or otherwise abuse the trust of its end-users. If a company is an information fiduciary, it has duties not to use the information it collects against its end-users in the ways described above. If it is inappropriate for a company to try to use collections of personal data to embarrass or manipulate end-users, the fact that it uses artificial intelligence or algorithms to do so hardly matters. Indeed, the fact that companies have increasingly powerful algorithms and artificial intelligence agents at their disposal means only that they have ever more power over their end-users, and therefore a greater responsibility to exercise appropriate care and loyalty.

The more interesting problem arises when algorithms use data about *other* people (or about large populations) in order to make predictions about users, and users have no relationship of trust or confidence with the enterprise that uses the algorithm. Examples are situations in

[171] *See, e.g.*, Nate Berg, *Predicting Crime, LAPD-Style*, GUARDIAN (June 25, 2014, 5:19 EDT), http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report (discussing police departments' use of algorithms to identify areas with high probabilities for certain types of crime); Natasha Singer, *Whether Working or Job Seeking, the Algorithm Is Watching*, N.Y. TIMES (Dec. 28, 2014, 5:20 PM), http://bits.blogs.nytimes.com/2014/12/28/whether-working-or-job-seeking-the-algorithm-is-watching/ (discussing companies' use of algorithms to monitor and rank both employees and job seekers). *See generally*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (discussing the role of algorithms in finance, search, advertising, and employment).

which we apply for credit;[172] or seek employment, housing, or business opportunities.[173] Companies will use algorithms and artificial intelligence to try to predict people's behavior in advance.[174] Their construction of social spaces and social opportunities will affect more than their base of end-users and clients.

When we are the end-user, client or customer of such a company, the problem of discrimination and manipulation arises out of an abuse of trust in the use of our personal information. But when we are not an end-user, client, or customer, there is no violation of a special relationship. Rather, the concern is about discrimination and manipulation that has effects on society in general. The Facebook story that begins this essay offers an example.[175] If a social media company attempted to swing a national election by manipulating its end-users, it would affect everyone in the population whether or not they used the service.

That is why the analysis I have offered in this essay can only take us so far. The concept of information fiduciaries presented here focuses on the violations of special relationships between companies and the people whose information they collect, collate, and use. To the extent that these companies take on fiduciary duties, they may also have duties to ensure that, when they sell or convey this information to others, duties of non-disclosure and non-manipulation travel with the data. But in the Algorithmic Society, companies will purchase and use lots of data that is not so encumbered, and they will use it to affect the lives of countless people who are not their clients or end-users.

At this point, we can no longer rely on the notion of special fiduciary relationships between individuals and companies to regulate the use and abuse of data. Instead, we must ask what duties of good

---

[172] *See, e.g.*, Amir E. Khandani, Adlar J. Kim & Andrew W. Lo, Consumer Credit Risk Models via Machine-Learning Algorithms 2 (May 9, 2010), *available at* https://mitsloan.mit.edu/media/Lo_ConsumerCreditRiskModels.pdf (describing an algorithm to predict consumer spending).

[173] *See, e.g.*, Tim Adams, *Job Hunting Is a Matter of Big Data, Not How You Perform at an Interview*, GUARDIAN (May 10, 2014, 4:00 EDT), http://www.theguardian.com/technology/2014/may/10/job-hunting-big-data-interview-algorithms-employees (describing "[t]he advance of algorithms into recruitment and 'talent management'"); Rachel Emma Silverman & Nikki Waller, *The Algorithm That Tells the Boss Who Might Quit*, WALL ST. J. (Mar. 13, 2015, 7:05 PM ET), http://www.wsj.com/articles/the-algorithm-that-tells-the-boss-who-might-quit-1426287935 (describing use of algorithms by Wal-Mart and Credit Suisse to decide which employees are likely to leave or stay).

[174] *See, e.g.*, Larry Hardesty, *Automating Big-Data Analysis*, MIT NEWS (Oct. 16, 2015), http://news.mit.edu/2015/automating-big-data-analysis-1016 (describing algorithms that predict human behavior better than experts).

[175] *See supra* Part II.

faith and ethical conduct in the collection, analysis, use, sale and distribution of data are owed to the members of society as a whole.[176] That is, our focus will shift from duties of confidentiality and loyalty to particular end-users to obligations of trustworthiness and fair play with respect to the general public. As we move from the world of the Internet to the Algorithmic Society, the horizons of our concern must expand accordingly.

[176] *Cf.* FRANKEL, *supra* note 106, at 3, 159-60, 167 (noting the possibility that courts may consider the needs of the public in articulating fiduciary duties between parties).