THE FIDUCIARY MODEL OF PRIVACY†

*Jack M. Balkin**

I. DIGITAL DEPENDENCE IN SURVEILLANCE CAPITALISM

In the digital age people are increasingly dependent on and vulnerable to digital businesses that collect data from them and use data about them. These companies use data to predict and control what end users do, and to sell advertisers access to those end users. Digital companies invite people to trust them with their data. When people accept that offer of trust, they become vulnerable: to how the companies use their data, to companies' data security (or lack thereof), and to companies' choice to share or sell the data to others. Because of the vulnerability and dependence created by information capitalism, I have argued that the law should treat digital companies that collect and use end user data according to fiduciary principles. The law should regard them as *information fiduciaries*.[1]

We rely on digital businesses to perform many different tasks for us. In the process, these businesses learn a lot about us — our likes, our dislikes, our habits, our movements, websites we visit, who we communicate with and when we do it, features of our bodies, even how we type on, click, and touch digital interfaces. Although digital companies know a lot about us, we do not know a lot about them — their operations, what kinds of data they collect, how they use this data, and who they share it with. Because of this asymmetry of information, we are especially vulnerable to them, and we have to trust that they will not betray our trust or manipulate us.[2]

---

† Responding to Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

* Knight Professor of Constitutional Law and the First Amendment, Yale Law School. My thanks to Woodrow Hartzog, David Pozen, Neil Richards, and Andrew Tuch for their comments on previous drafts.

[1] *See* Jack M. Balkin, Lecture, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1221 (2016) [hereinafter Balkin, *Information Fiduciaries*]; Jack M. Balkin, Essay, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2048 (2018) [hereinafter Balkin, *Free Speech Is a Triangle*]; Jack M. Balkin, Essay, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1162 (2018) [hereinafter Balkin, *Algorithmic Society*].

[2] In my work on information fiduciaries, I define manipulation as "techniques of persuasion and influence that (1) prey on another person's emotional vulnerabilities and lack of knowledge (2) to benefit oneself or one's allies and (3) reduce the welfare of the other person." Jack M. Balkin, *Fixing Social Media's Grand Bargain* 4 (Hoover Working Grp. on Nat'l Sec., Tech. & L., Aegis Series Paper No. 1814, 2018), https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf [https://perma.cc/774R-AD7D].

The problem is not simply asymmetry of information. Many companies design their interfaces to facilitate and encourage the disclosure of information, including information we may not even be aware we are disclosing. Simply moving around a city with a cell phone or other digital device may produce lots of information about us.[3] Social media companies like Facebook design their interfaces to make it difficult to protect our privacy, burying privacy settings and making them confusing.[4] They also use algorithms to monopolize our attention and keep us fixed to the site so that we will disclose even more information. Some companies have even taken a cue from casinos in figuring out how to addict their audiences.[5]

Thus, in addition to information asymmetry and lack of transparency, there is the asymmetry in power that occurs because one party controls the design of applications and the other must operate within that design. There is always a danger of manipulation after the data is collected. But there is also manipulation before the fact, in the design of interfaces and services to encourage data sharing and hide the consequences of our choices and actions.

In the midst of these asymmetries of knowledge, power, and control, digital companies hold themselves out as trustworthy enterprises; they insist that our data is safe with them and that our privacy and our safety is their central concern. They encourage us to trust them so that we will entrust them with our data, indeed, with our digital lives.

And we do entrust them with our data. It is increasingly difficult to avoid dealing with digital companies that collect and use our data. Cell phone companies, broadband providers, social media companies, search engines, platform businesses like Uber, Airbnb, and Instacart, health and fitness applications like Fitbit, games like Pokémon GO and Fortnite, video-meeting applications like Zoom, streaming services like

---

[3] *See, e.g.*, Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://nyti.ms/3a5VCbp [https://perma.cc/7KQG-X3MB].

[4] *See, e.g.*, Rebecca Greenfield, *Facebook Privacy Is So Confusing Even the Zuckerberg Family Photo Isn't Private*, THE ATLANTIC (Dec. 26, 2012), https://www.theatlantic.com/technology/archive/2012/12/facebook-privacy-so-confusing-even-zuckerberg-family-photo-isnt-private/320164 [https://perma.cc/QE3H-322L].

[5] *See, e.g.*, Vivek Wadhwa, *Workplace Technology Is as Addictive as a Casino's Slot Machine — And Makes Us Less Productive*, MARKETWATCH (July 30, 2018, 8:48 AM), https://www.marketwatch.com/story/workplace-technology-is-as-addictive-as-a-casinos-slot-machine-and-makes-us-less-productive-2018-07-30 [https://perma.cc/K95L-ZFDJ]; Mattha Busby, *Social Media Copies Gambling Methods "to Create Psychological Cravings,"* THE GUARDIAN (May 8, 2018, 2:00 AM), https://www.theguardian.com/technology/2018/may/08/social-media-copies-gambling-methods-to-create-psychological-cravings [https://perma.cc/BQ5V-7BCB]; Julian Morgans, *The Secret Ways Social Media Is Built for Addiction*, VICE (May 21, 2017, 4:30 AM), https://www.vice.com/en_uk/article/vv5jkb/the-secret-ways-social-media-is-built-for-addiction [https://perma.cc/Z8SB-7TU4].

Hulu, Disney+, and Netflix — each of these companies collects data about us and our experiences as they provide us with different kinds of services. To live without interacting with any of these services means greatly constricting one's life and opportunities, because the most ordinary tasks — finding a job, commuting from place to place, procuring food, staying in touch with friends and relatives, accessing news and information — expose us to surveillance and data collection. The COVID-19 pandemic accelerated existing trends in which we live much of our lives online, with many experiences and relationships mediated by digital companies that collect information about us as a consequence of using their services.[6]

These dependencies will only increase over time. Personal digital assistants like Alexa and Siri (soon to be followed by personal robots[7]) are in our homes and offices waiting for our commands, in exchange for ever more data about our desires and habits, even the emotional inflection of our voices.[8] The rapidly growing internet of things promises to make almost every appliance we interact with a data collection device, the better to serve us — and monitor us.[9] Businesses want us to depend more and more on these technologies; indeed, they want our dependence to be second nature, so that someday we would not even think of doing without them.

A. The Fiduciary Model

The law recognizes fiduciary relationships for precisely these kinds of situations. In general, the law looks to whether the stronger party has issued an implicit or explicit invitation to trust that the weaker party has accepted.[10] It looks to factors including an imbalance of power, a

---

[6] *See* Yan Xiao & Ziyang Fan, *10 Technology Trends to Watch in the COVID-19 Pandemic*, WORLD ECON. F. (Apr. 27, 2020), https://www.weforum.org/agenda/2020/04/10-technology-trends-coronavirus-covid19-pandemic-robotics-telehealth [https://perma.cc/K7ZK-HMKJ].

[7] *See, e.g.*, Mark Gurman, *Amazon Is Building a Voice-Controlled Robot That's Like a "Mobile Alexa,"* TIME (July 12, 2019, 2:51 PM), https://time.com/5625636/amazon-alexa-echo-voice-robot [https://perma.cc/D8BM-AKCY].

[8] *See, e.g.*, Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to that Data?*, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice [https://perma.cc/2WM7-DEDZ].

[9] *See* LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 59–93 (2020).

[10] *See* Eileen A. Scallen, *Promises Broken vs. Promises Betrayed: Metaphor, Analogy, and the New Fiduciary Principle*, 1993 U. ILL. L. REV. 897, 901, 922, 926–27, 953 (arguing that a fiduciary duty exists when the stronger party issues an invitation to trust and the trusting party cannot adequately protect itself because of its dependence or vulnerability); Neil Richards & Woodrow Hartzog, A Duty of Loyalty for Privacy Law 48 (Sept. 5, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217 [https://perma.cc/4D28-8QMN] ("Drawing from lessons of fiduciary and confidentiality law, we identify four conditions that, when present, should give rise to a duty of loyalty: (1) When trust is invited; (2) From people made vulnerable by

significant asymmetry of knowledge, the weaker party's practical inability to supervise, control, or monitor the more powerful party, the weaker party's dependence on the more powerful party, and the consequent vulnerability that comes with the need to trust.[11] Fiduciary obligations go beyond the ordinary obligation of good faith that applies to all commercial transactions. They are duties of care, confidentiality, and loyalty toward those our invitation to trust has placed in special positions of vulnerability.[12]

Information fiduciaries have three basic kinds of duties toward their end users: a duty of confidentiality, a duty of care, and a duty of loyalty.[13] The duties of confidentiality and care require digital companies to keep their customers' data confidential and secure. These fiduciary duties also must "run with the data"[14]: digital companies "must ensure that anyone who shares or uses the data is equally trustworthy and is legally bound by the same legal requirements of confidentiality, care, and loyalty" as they are.[15] Digital companies "must vet . . . potential partners to make sure that they are ethical and reliable, subject them to regular audits, and, if [partners] violate the terms of their agreements, [digital companies] must take steps to get back . . . the data" they shared.[16] The duty of loyalty means that digital companies may not manipulate end users or betray their trust.[17] Companies must act in the interests of the end users whose data they collect, and they must design their systems to avoid creating conflicts of interests with their end users — for example, by promoting addictive behavior.[18]

Requiring that duties run with the data brings into the system of trust a range of other companies that do not deal directly with end users but may affect their well-being. When digital-information fiduciaries

---

exposure; (3) When the trustee has control over peoples' online experiences and data processing; and (4) When people trust data collectors with their exposure.").

[11] *See* Paul B. Miller, *The Identification of Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 367, 374 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) (listing factors relevant to fiduciary relationships); TAMAR FRANKEL, FIDUCIARY LAW xvi, 4, 6, 18, 29 (2011) (noting that asymmetries of knowledge and power characterize most fiduciary relationships).

[12] *See* Daniel B. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 11, at 3, 13; *see also* Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 882 (explaining that "[t]he fiduciary's duties go beyond mere fairness and honesty; they oblige him to act to further the beneficiary's best interests").

[13] Balkin, *Information Fiduciaries*, *supra* note 1, at 1206–08; Balkin, *Free Speech Is a Triangle*, *supra* note 1, at 2048.

[14] Balkin, *Free Speech Is a Triangle*, *supra* note 1, at 2051.

[15] *Id.* at 2052.

[16] *Id.*

[17] *See id.* at 2052–53.

[18] *See id.*

make deals or share data with data brokers or other surveillance companies, they must demand and enforce fiduciary protections for their end users. If an information fiduciary allows a third party to place trackers or other surveillance code on its website or application, the third party must agree to assume fiduciary duties with respect to the data collected and used. And all apps on a platform that use the platform to collect data from the platform's end users, or that share or leverage data collected by the platform, must promise the platform that they will act as information fiduciaries with respect to the data they collect and use.

In other writings I have analogized the duties of information fiduciaries to the duties that professionals like doctors and lawyers have to their patients and clients.[19] People need to trust their doctors and lawyers with sensitive personal information that could easily be used against them. Because of asymmetries of information and power in these professional relationships, the law treats doctors and lawyers as fiduciaries.[20]

But in making these analogies, we should not forget a central point: fiduciary obligations arise out of social relationships, and the power and vulnerability inherent in these relationships.[21] The nature of fiduciary obligations depends on the nature of the relationship, the understandings of the participants, and the potential dangers of abuse, manipulation, self-dealing, and overreaching by the more powerful party.[22]

Digital companies like Facebook do not perform the same kind of services that doctors and lawyers offer.[23] On the one hand, people expect very different things from these companies than they do from their doctors and lawyers. Social media companies are not trained professionals that we expect will attend to our health or our legal problems. They are communications technologies for social interaction, entertainment, and news. On the other hand, Facebook has the ability to collect far more information of different kinds about us than any physician or lawyer ever could.[24] And it has at its disposal computational power and artificial intelligence capacities to make predictions and engage in forms of manipulation that doctors and lawyers have never possessed. These

---

[19] *See, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 1, at 1205–08.

[20] FRANKEL, *supra* note 11, at 42–45 (offering a list of traditional fiduciaries including professionals like doctors and lawyers).

[21] *See* Balkin, *Information Fiduciaries*, *supra* note 1, at 1205.

[22] Tamar Frankel, *Fiduciary Law*, 71 CALIF. L. REV. 795, 810 (1983) ("Fiduciary relations vary by the extent to which each type of fiduciary can abuse his power to the detriment of the entrustor.").

[23] *See* Balkin, *Free Speech Is a Triangle*, *supra* note 1, at 2049.

[24] *See id.*

differences mean that while the fiduciary obligations of digital companies may be different and narrower than the obligations of professionals, they may be just as important.

B. Privacy and Trust

The information-fiduciary model is an instance of a larger trend in theories of digital privacy — a movement to viewing privacy in relational terms of trust and trustworthiness. These theories focus on questions of loyalty, disparities of power, and vulnerability.[25]

Theories that emphasize privacy-as-trust and privacy-as-loyalty differ from earlier theories of privacy based on the model of fair information practices — a model which, in its most stripped-down version, focuses on notice to end users and end-user choice.[26]

Notice-and-choice approaches to privacy have well-known problems. First, end users lack the ability to assess the risks of future harm from the collection, use, and disclosure of their data. Even if they read a company's privacy policies (which few people do[27]), they may be unaware of the many different kinds of data that companies can extract from them and the many different kinds of uses to which their data can be put.

Second, end users cannot easily tell how their data may be combined with other data in the future to draw surprising and powerful inferences about them that might be used to their detriment. Because people cannot easily assess the value of what they are giving up or the risk of future harms, we cannot assume that their decisions are truly informed or are likely to maximize their welfare.

Third, digital companies create the environment in which end users operate. They can structure the very conditions of choice. And without end users even being aware of it, companies can design interfaces to maximize data collection and induce disclosure.

---

[25] *See, e.g.*, ARI EZRA WALDMAN, PRIVACY AS TRUST 61–76 (2018); DANIEL J. SOLOVE, THE DIGITAL PERSON 103 (2004); Richards & Hartzog, *supra* note 10; Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1 (2018); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 340–41 (2014); Ian Kerr, *Personal Relationships in the Year 2000: Me and My ISP*, *in* RELATIONSHIPS OF DEPENDENCE AND INTERDEPENDENCE IN LAW 78, 110–11 (2002); Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?*, 81 B.U. L. REV. 635 (2001); Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419 (2001).

[26] *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 960, 975 (2017); Richards & Hartzog, *supra* note 25, at 444–45.

[27] Kim Hart, *Privacy Policies Are Read by an Aging Few*, AXIOS (Feb. 28, 2019), https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html [https://perma.cc/9CDE-WWEW].

Fourth, because companies control the end user's environment, they can leverage the emotions and cognitive limitations of end users not only to induce disclosure but also to shape behavior.

Fifth, the data that companies gather from end users can have significant external effects on third parties who may not even be users of the site. As digital companies know more about a given person, they can also know more about other people who are similar to that person or are connected to that person. In the digital age, everyone is always informing on everyone else. Thus, an individual's response to a notice-and-choice regime may affect the privacy of many other people who have no say in the matter. And when companies manipulate end users' moods and decisions — including their decisions to vote — they affect not only particular end users but many other people as well.

Notice-and-choice models are most inadequate when end users are most vulnerable, and when asymmetries of knowledge, power, and control are greatest. Put another way, notice-and-choice models of privacy are the most inadequate under precisely the conditions that define surveillance capitalism. That is why we need the fiduciary model.

C. The Fiduciary Model's Systemic Effects

Because the traditional fiduciary concept involves relations of trust between individuals, people may overlook the systemic impact that a fiduciary model of privacy would have if governments took it seriously and implemented it thoroughly in digital environments.[28]

First, the fiduciary model applies not only to large social media platforms like Facebook but also to all businesses that collect information from end users in return for services, whether or not the end user pays fees or has a subscription. This formula includes all businesses that barter end-user data for purportedly "free" services, because all such relationships are effectively agreements with end users for valuable data. The fiduciary model thus includes people's broadband and cell phone companies, their email provider, their game and entertainment platforms, and all internet-of-things appliances, services, and artificial intelligence agents they employ in their daily lives. For the same reason, the fiduciary model will also encompass robots, self-driving cars, and companies that provide virtual- or augmented-reality environments.

Second, as noted above, whenever an information fiduciary shares data with a third party, fiduciary duties must run with the data. This means that data brokers that have no contractual relations with end users may still be bound by fiduciary obligations. That is because if they collect information from multiple sources, including from information fiduciaries, they will have to enter into privacy agreements with

---

[28] *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 528, 535 (2019).

each information fiduciary. Because, as time goes on, and data is analyzed, collated, and repurposed, it will be very difficult for data brokers to know which data they collect comes with fiduciary obligations and which does not, they will be driven to treat all the data they collect in the same way, or else risk liability or government sanction. Although the fiduciary model does not appear at first glance to touch data brokers at all, it will revolutionize their practices.

Third, large platforms like Facebook, Google, and Amazon have so many end users that a requirement that they must act in the interests of their end users effectively requires them to act in the interests of the public as a whole. Thus it would violate Facebook's fiduciary duties of care and loyalty to manipulate end users to vote for candidates of Facebook's liking or not to vote at all.[29] Facebook also has a fiduciary duty to its end users not to allow data about its end users (and thus algorithms built on that data) to be used to spread public health disinformation, even if a nonfiduciary would be allowed to spread such disinformation. This duty to end users benefits the public as a whole.[30]

Fourth, as noted above, decisions to disclose data have significant third-party effects. When I offer my data to a digital company, I also reveal information about everyone who is connected to me or similar to me. For that reason, the fiduciary model dovetails with models that treat privacy as an environmental problem like pollution.[31]

D. The Fiduciary Model and the Fourth Amendment

The fiduciary model also helps secure greater Fourth Amendment protection from government searches and seizures. Under the third-party doctrine, people have no expectation of privacy in data held by

---

[29] *Cf.* Zittrain, *supra* note 25, at 335–38; Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), http://www.newrepublic.com/article/117878/informationfiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/3FUN-W2K9].

[30] Congress may add additional public interest obligations in exchange for intermediary immunity. *See infra* section V.B, pp. 32–33.

[31] *See* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1742–45 (comparing privacy invasions to physical pollution); Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 112–13 (2019) (analogizing privacy harms to environmental harms); Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 23 (2006) (arguing that "[t]he privacy injuries of the Information Age are structurally similar to the environmental damage of the smokestack era" because of negative externalities and problems of collective action). In previous work, for example, I have developed the concept of "algorithmic nuisance," which maintains that companies must internalize the social costs of algorithmic decisionmaking on society. Jack M. Balkin, Lecture, *2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1232–40 (2017) [hereinafter Balkin, *Three Laws*]; Balkin, *Algorithmic Society*, *supra* note 1, at 1163–68.

third parties — which includes all the data collected by digital companies.[32] Therefore governments can obtain this information without a warrant.[33] The Supreme Court has begun to recognize that the third-party doctrine makes little sense in the digital age and is slowly moving away from it.[34] The fiduciary model offers a clear path forward. If a digital business is an information fiduciary — as cell phone and social media companies are, for example — people have a reasonable expectation in the fiduciary's duty of confidentiality.[35] That means that a warrant is normally required to access nonpublic data about end users.[36]

The fiduciary model does not abolish the third-party doctrine. It merely limits its application to those persons and businesses who are not our information fiduciaries. It provides a tractable set of questions to decide when the third-party doctrine applies to digital businesses. The fiduciary model also helps stabilize the often-criticized *Katz*[37] test of reasonable expectations of privacy. Under the fiduciary model, the question is not whether consumers reasonably expect that a particular type of data will be kept private. Rather, the question is whether the relationship between end users and digital companies is a fiduciary relationship of trust. If so, then the question becomes whether the digital business can freely disclose this information to others consistent with their fiduciary obligations. If not, then the government needs to obtain a warrant. The fiduciary model helps preserve our security from the government as we hand over more and more information about ourselves to digital businesses. It prevents our constitutional rights from continually contracting in the digital age. This security is especially important because government increasingly seeks to enlist the privately owned infrastructure of communication to help the government engage in surveillance of its citizens.[38]

Moreover, under the fiduciary model, digital businesses have an affirmative obligation to defend and protect the privacy of their end users, not only from other private entities, but also from the prying eyes of the

---

[32] *See* United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that there is no expectation of privacy in information voluntarily turned over to third parties); *see also* Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that there is no expectation of privacy in metadata collected as a result of making a phone call).

[33] *See Smith*, 442 U.S. at 746; *Miller*, 425 U.S. at 444.

[34] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (holding that the third-party doctrine excludes cell-site location information).

[35] *See* Balkin, *Information Fiduciaries*, *supra* note 1, at 1230–31.

[36] *See id.*; Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 659 (2015) (arguing that the misplaced-trust rule should not apply to information fiduciaries).

[37] Katz v. United States, 389 U.S. 347 (1967).

[38] Balkin, *Free Speech Is a Triangle*, *supra* note 1, at 2019–20, 2029; Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298–99, 2305 (2014).

government.[39] Some digital businesses, like Apple, already see it as in their interest to defend personal data from government intrusion.[40] The fiduciary model treats this approach as more than simply good public relations; it is required by the duties of care, confidentiality, and loyalty to end users.

II. ANTITRUST SHOULD NOT BE ANTI-TRUST

By the end of their critique of the information-fiduciary model, Professors Lina Khan and David Pozen make their real concerns clear: the central problem we face today is the economic power of digital platforms.[41] Fix platform power and it will ameliorate not only privacy problems but also many other problems as well. Privacy reforms like the fiduciary model divert scarce political attention and capital from the real issue: combatting the concentrated power of today's digital giants.[42] In fact, large digital businesses would probably prefer that Congress spend its time on proposals that make them information fiduciaries, because this would leave the real sources of companies' power — and their power to do harm — unaddressed.[43]

I agree that reform of digital businesses must focus on platform power. I also agree that the problems are structural, and that structural reforms are necessary. Near the end of their article, Khan and Pozen recognize that I have repeatedly written in favor of antitrust regulation and competition policy as crucial elements of reform.[44] As Khan and Pozen well know, I am a fox, not a hedgehog.

To the extent we have any disagreements, they are twofold. First, I think they undersell how fiduciary models of privacy, taken seriously, will alter digital business models and require companies to change their existing ways of doing business.

---

[39] *See* MIKE GODWIN, THE SPLINTERS OF OUR DISCONTENT: HOW TO FIX SOCIAL MEDIA AND DEMOCRACY WITHOUT BREAKING THEM 29–38 (2019).

[40] *See, e.g.*, Stephen L. Carter, *Apple's Case Against the FBI Is Stronger than Ever*, BLOOMBERG (Jan. 10, 2020, 9:30 AM), https://www.bloomberg.com/opinion/articles/2020-01-10/apple-should-keep-denying-fbi-requests-to-crack-iphones [https://perma.cc/XDQ3-DBRX].

[41] *See* Khan & Pozen, *supra* note 28, at 502, 528, 540–41.

[42] *See id.* at 537, 540–41.

[43] *See id.* at 528, 537.

[44] *See id.* at 536; *see also* Balkin, *Free Speech Is a Triangle*, *supra* note 1, at 2034–36 (arguing for antitrust and competition reforms to change business models and promote democracy); Balkin, *supra* note 2, at 10–11, 15 (arguing for using antitrust and competition law to change business models, eliminate perverse incentives, and promote democracy); Jack M. Balkin, *How to Regulate (and Not Regulate) Social Media*, KNIGHT FIRST AMEND. INST. (Mar. 25, 2020), https://knightcolumbia.org/content/how-to-regulate-and-not-regulate-social-media [https://perma.cc/H3SH-FYB5] (arguing for antitrust and competition law solutions).

Second, I think that we have no choice but to proceed on multiple fronts.[45] The power of digital businesses, and the problems they cause, arose from multiple changes in law during the Second Gilded Age, in fields ranging from intellectual property law to consumer protection and privacy law, telecommunications law, First Amendment law, antitrust law, and competition policy.[46] To respond to the problems, we will have to push for reforms in many areas. I agree that attending *only* to privacy reform will leave crucial problems of economic concentration unaddressed. But that is neither my approach nor my purpose. And the converse is also true. Focusing solely on antitrust and competition policy may not solve — or may even exacerbate — important threats to digital privacy.

Here is a simple example: I have argued for a requirement of "adversarial interoperability"[47] along the lines laid out by Mike Masnick and Cory Doctorow.[48] Network effects make it very difficult to combat platform power, especially in social media. People join Facebook and submit to its privacy abuses because everyone else has joined Facebook. But if we require platforms to make their application protocols available, programmers can create feeds of multiple social media. (Ethan Zuckerman's team at the MIT Center for Civic Media has created an application that consolidates feeds across applications in just this way.[49]) Opening up protocols allows more social media companies with different features, affordances, rules, and curation practices, because it makes it easier for people to try out different platforms and move easily between them.

---

[45] Balkin, *supra* note 44 (arguing for using multiple policy levers of antitrust, competition, privacy, consumer protection, and telecommunications law).

[46] *See generally* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019) (analyzing how legal institutions have transformed in the digital age); Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1480–97 (2020) (reviewing COHEN, *supra*).

[47] Jack M. Balkin, Professor, Yale L. Sch., Remarks at Floyd Abrams Institute for Freedom of Expression Panel: Where Algorithms Meet the First Amendment, at 48:15, YOUTUBE (June 2, 2020), https://www.youtube.com/watch?v=V5DbtWhYPzw [https://perma.cc/9QAU-96G3] (arguing for adversarial interoperability and reform of the Computer Fraud and Abuse Act).

[48] *See, e.g.*, Cory Doctorow, *Adversarial Interoperability*, EFF (Oct. 2, 2019), https://www.eff.org/deeplinks/2019/10/adversarial-interoperability [https://perma.cc/SA78-UEPN]; Cory Doctorow, *Adversarial Interoperability: Reviving an Elegant Weapon from a More Civilized Age to Slay Today's Monopolies*, EFF (June 7, 2019), https://www.eff.org/deeplinks/2019/06/adversarial-interoperability-reviving-elegant-weapon-more-civilized-age-slay [https://perma.cc/C9UE-JPXR]; Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, KNIGHT FIRST AMEND. INST. (Aug. 21, 2019), https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech [https://perma.cc/4QCG-K32L].

[49] *See* Anna Woorim Chung, *Gobo: Your Social Media, Your Rules*, MIT CTR. FOR CIVIC MEDIA (June 3, 2019), https://civic.mit.edu/2019/06/03/gobo-your-social-media-your-rules [https://perma.cc/2S9B-LR62]. Implementing Zuckerman's vision would require amending the Computer Fraud and Abuse Act, which exemplifies my point that cyberlaw and intellectual property law reforms as well as antitrust and privacy reforms are needed.

But interoperability creates a privacy problem. The more easily data can be shared, the greater the danger that someone who gets a hold of it will misuse it. The more entrants there are in the social media market, therefore, the more important it is that each of them accepts fiduciary obligations. Here is another way to see the point: even if we broke up Facebook tomorrow into fifty little Facebooks, each of them would still be practicing surveillance capitalism. Smaller companies may be economically less powerful, but they may still be able to surveil and manipulate their end users, especially if information is still asymmetric and end users don't understand how digital businesses work. Because the vast majority of end users are essentially clueless, more competition won't end all abusive privacy practices. We need fiduciary obligations as well as competition law reforms.

If digital antitrust advocates allow themselves to become the adversaries of privacy reform, neither cause will be well served. The goal of the fiduciary models is to require digital companies, which are not trustworthy stewards of the data they collect and use, to become trustworthy and look out for the interests of end users. To quote Professor Neil Richards, there is no reason why antitrust should be anti-trust.[50]

I am more optimistic than Khan and Pozen that pushing for consumer protection and privacy reforms will not crowd out demands for renewed antitrust enforcement and competition law reforms. In fact, as is often true of social mobilizations, different demands for reform can build on each other. Right now we are in the darkest days of a Second Gilded Age. But recent popular mobilizations for economic and racial justice herald the potential for a Second Progressive Era to follow. If the political will emerges to seriously rethink digital capitalism, it will likely occur on multiple fronts at once, much as it did with industrial capitalism in the First Progressive Era and later, the New Deal.

Khan and Pozen's concern that privacy reforms will waste political capital is not an argument about either law or policy, but about political strategy, a question on which none of us are experts. Their guess as to what will happen in the future is as good as mine, which means that my guess is as good as theirs.

III. CRITIQUES OF THE INFORMATION-FIDUCIARY MODEL

A. Sorry About Your Privacy: We Need to Make Profits!

Khan and Pozen's central argument against the information-fiduciary model is that making corporations information fiduciaries will

---

[50] Interview with Neil Richards, Professor, Wash. Univ. in St. Louis, in Palo Alto, Cal. (Mar. 19, 2019).

conflict with management's existing fiduciary duties to shareholders.[51] The information-fiduciary approach cannot work as a logical matter because it requires divided loyalties.[52]

This criticism seems misguided. First, Khan and Pozen concede that there is no problem of divided loyalties if legal obligations to protect privacy take precedence over management's duty to maximize shareholder value.[53] A federal privacy statute that includes information-fiduciary obligations would preempt (Delaware) state law to the contrary.[54] Problem solved.

Second, even putting preemption to one side, the argument rests on a faulty premise. Corporations could make a lot more money for their shareholders if they could dump pollutants in rivers, bamboozle customers, and conspire to fix prices. But Khan and Pozen do not argue that consumer protection law, environmental law, or antitrust law are logically incoherent and unenforceable because they conflict with management's duty to maximize shareholder value. Management's fiduciary obligations to shareholders *assume* that the corporation will attempt to comply with the legal duties owed to those affected by the corporation's business practices, even if this reduces shareholder value.[55]

The central problem that gives rise to fiduciary obligations in corporate law is the separation of ownership from control, and the difficulty of supervising and controlling management.[56] Fiduciary obligations prevent management from wasting the corporation's assets, diverting these assets to management's benefit, or engaging in other forms of self-dealing.[57] But legal obligations that require corporations — like all other businesses — to internalize the social costs they impose on other actors normally do not activate these concerns, so these legal obligations normally do not conflict with management's fiduciary duties to shareholders.[58] Moreover, the business judgment rule in Delaware gives management wide discretion to decide how best to employ the corporation's

---

[51] *See* Khan & Pozen, *supra* note 28, at 504.

[52] *Id.*

[53] *See id.* at 509.

[54] *See id.*

[55] Indeed, management's duty of loyalty to shareholders *requires* directors to make good faith efforts to ensure that the corporation complies with all regulatory laws that apply to its operations. *See* Marchand v. Barnhill, 212 A.3d 805, 820–21 (Del. 2019); *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996).

[56] *See, e.g.*, Larry E. Ribstein, *Fencing Fiduciary Duties*, 91 B.U. L. REV. 899, 901 (2011); Robert Cooter & Bradley J. Freedman, *The Fiduciary Relationship: Its Economic Character and Legal Consequences*, 66 N.Y.U. L. REV. 1045, 1048 (1991).

[57] *See, e.g.*, Julian Velsaco, *Fiduciary Principles in Corporate Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 11, at 61, 66–69.

[58] *See* ROBERT CHARLES CLARK, CORPORATE LAW 18 (1986) (explaining that management's duty is to "maximize the value of the company's shares, subject to the constraint that the corporation must meet all its legal obligations to others who are related to or affected by it").

assets in the interests of shareholders.[59] Khan and Pozen are not arguing that corporations violate their fiduciary obligations to shareholders when they guarantee end users privacy, confidentiality, and data security in their terms of service.

Indeed, Goldman Sachs, Blackrock, and a host of other financial services corporations would be very surprised to learn that they cannot have fiduciary duties to their nonshareholder customers, or that there are no plausible ways of mitigating potential conflicts of interest.[60] Like the old joke about baptism, I not only believe it, I've seen it done.

Perhaps what Khan and Pozen mean is that the duties of care, confidentiality, and loyalty are vague standards and so it will be difficult to predict when fiduciary duties to end users will lower shareholder value. Of course many legal obligations involve vague standards, including the reasonable person standard and the concept of a product defect in tort law. If vagueness is the concern, the answer is to use either common law decisionmaking (as in antitrust and products liability) or rulemaking and adjudication by administrative agencies to articulate privacy obligations in more concrete rules and standards. If the federal government includes the fiduciary model in comprehensive privacy regulation, it should delegate this task to a federal agency.[61]

I suspect that what Khan and Pozen are really getting at is that fiduciary obligations to end users will require today's digital corporations to change their existing business models. By (finally) putting end users first, they will have to put corporate profits second. Khan and Pozen argue that advocates of the fiduciary model have not been sufficiently candid about this.[62] (They do not accuse me of any lack of candor.) They tell us that their critique will be a "(partial) success"[63] if advocates make clear that making digital businesses information fiduciaries will require "sacrificing stockholders' economic interests to advance users' noneconomic interests"[64] in privacy. To which I can only reply: Congratulations, your article is a success!

---

[59] *See* Unocal Corp. v. Mesa Petroleum Co., 493 A.2d 946, 954 (Del. 1985) ("A hallmark of the business judgment rule is that a court will not substitute its judgment for that of the board if the latter's decision can be 'attributed to any rational business purpose.'" (quoting Sinclair Oil Corp. v. Levien, 280 A.2d 717, 720 (Del. 1971))).

[60] *See* Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. (forthcoming 2021) (manuscript at 5), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3696946 [https://perma.cc/5AXA-NBJD] ("Many of the largest financial services firms are subject to fiduciary regimes that arguably impose dual loyalties, as the information fiduciary model might.").

[61] *See* Khan & Pozen, *supra* note 28, at 522, 524–26 (asking whether I support such agency enforcement, *id.* at 524). Yes, I do.

[62] *See id.* at 508.

[63] *Id.* at 509 n.58.

[64] *Id.*

B. Facebook Is Not Your Doctor. It's Even Scarier than Needles.

Khan and Pozen's next argument is that there are important disanalogies between digital companies and professionals like doctors and lawyers. First, unlike doctors and lawyers, digital businesses like Facebook use their expertise to make end users more vulnerable.[65] Second, patients understand that they are in a doctor-patient relationship with their physicians. But end users do not understand the real nature of their relationship with digital companies; they do not fully understand that they are the product.[66] Third, the economic livelihood of doctors is not in direct conflict with their treatment of their patients, while under current business models digital businesses make more money if they can manipulate their end users.[67] (This may somewhat overstate the case, because doctors' practices are often affected by insurance companies, who want to maximize profits and who may not have patients' best interests at heart.)

Fourth, doctors and lawyers collect data about their patients and clients that is in rough proportion to the services they provide.[68] But today's digital companies collect as much data as possible, far more than necessary to provide social media services or search-engine services[69] — to take two examples. Professor Shoshana Zuboff makes a similar point. Originally, Google used data from searches to improve search efficiency for end users. But the amount of data recovered, euphemistically called "data exhaust," was far greater.[70] The key moment in the rise of surveillance capitalism, Zuboff explains, was when Google began to monetize this "data exhaust" by using it to sell advertising to third parties.[71] Nothing like this occurs in the professions. Doctors do not use their interactions with patients as an opportunity to serve targeted ads by third parties.[72]

These disanalogies to the professions do not undermine the fiduciary model. They strengthen it. Fiduciary obligations arise from social

---

[65] *Id.* at 517–18.

[66] *Id.* at 519–20.

[67] *Id.* at 512–15.

[68] *See id.* at 517.

[69] *Id.* at 517–18.

[70] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 68 (2019).

[71] *Id.* at 78.

[72] *See* Khan & Pozen, *supra* note 28, at 514 & n.8. There is a fifth disanalogy that Khan and Pozen do not mention. Doctors and lawyers have developed professional codes of conduct designed to limit their misbehavior. But digital businesses — which come in many different varieties — have not done so. Facebook's Oversight Board for Content Decisions, for example, concerns only Facebook. Moreover, it focuses only on complaints about content moderation. At least at present, it leaves untouched the "crown jewels" — Facebook's data collection and surveillance practices — which are the source of its profits. Balkin, *supra* note 44.

relations of unequal power and vulnerability. Khan and Pozen are arguing that end users are potentially even *more* vulnerable to digital companies than they are to members of traditional professions. They are vulnerable because digital businesses repeatedly invite end users to trust them and end users are mostly unaware of the dangers. The logic of fiduciary obligations holds that the greater the imbalance of power, the greater the asymmetries of information, the greater the degree of control over the client's environment, and the greater the client's vulnerability, the greater the need for fiduciary obligations becomes. It can hardly be a good argument to oppose new fiduciary obligations where businesses are more predatory and consumers are less informed and more vulnerable to manipulation.

The argument might be that fiduciary obligations are futile because manipulation is baked into the business model.[73] But that would be like opposing the New Deal Securities Acts because the financial sector of the 1920s relied heavily on misleading investors, or opposing the Pure Food and Drug Act of 1906 because the turn-of-the-century meat processing industry relied on unsafe working conditions and the market for drugs was full of quack remedies. The whole point of the fiduciary model, in conjunction with competition law, is to *change* the business models of these companies, and to make them trustworthy stewards of personal data, as they currently claim they are, but actually are not.

Khan and Pozen assert that advocates of the fiduciary model believe that digital companies like Facebook and Google are already trustworthy companies that just need a little policing around the edges.[74] But that is not the point of the fiduciary model. These companies hold themselves out as trustworthy, but they are actually not trustworthy. They induce trust from end users, but they also betray it. The point of the model is to hold these companies to fiduciary obligations, not to pretend that they already have fulfilled them. It is to alter their ways of doing business, just as federal regulation transformed the securities industry, food industry, and the practice of medicine during the Progressive Era and the New Deal.

Following Professor Julie Cohen, Khan and Pozen raise the interesting question of whether fiduciary obligations are even possible where interactions are mediated by algorithms.[75] Classic fiduciaries, Cohen points out, operated on a human scale, at human speeds between human

---

[73] Khan & Pozen, *supra* note 28, at 515.

[74] *Id.* at 534 (claiming that the fiduciary model "characterizes Facebook, Google, Twitter, and other online platforms as fundamentally trustworthy actors who put their users' interests first").

[75] *Id.* at 514 n.81 (quoting Julie E. Cohen, *Scaling Trust and Other Fictions*, L. & POL. ECON. (May 29, 2019), https://lpeblog.org/2019/05/29/scaling-trust-and-other-fictions [https://perma.cc/C65Z-75J3]).

beings who were intelligible to each other.[76] Today, by contrast, we are ruled by instantaneous computer programs, which operate at scale and instantaneous speed, which are not intelligible to us, and which have no human relationships to us.[77]

This objection also proves too much. More and more of medicine makes use of algorithms and robotics.[78] The same is true of investment advice.[79] I would not take these developments as a reason to abandon fiduciary obligations for doctors or estate managers. Technology mediates and constitutes social relations between human beings, and technological change allows for new relationships of power and control. We always need to look behind the form of technology to the social relations of inequality and domination that a given technology allows and fosters.[80] If algorithms become technologies by which human beings can mistreat other human beings and deny responsibility for doing so, we should impose duties on the human beings and the companies they run who wield these technologies.[81]

C. But What About Targeted Advertising?

At bottom, Khan and Pozen do not believe that a fiduciary model is possible — or that it will be empty and toothless — because I have stated that digital businesses can still make money by serving targeted ads to end users.[82] For Khan and Pozen, this practice is simply a bridge too far: the ability to target ads at end users makes the conflicts of interest between digital companies and end users too great. It encourages companies to extract as much data as possible in order to make as much money as possible from advertising, whether or not this is in the best interests of end users.[83]

This conclusion does not follow unless we assume that all targeted advertising is inherently abusive and inconsistent with the best interests of end users. Since much of modern advertising is based on increasing efficiencies in locating and reaching interested audiences, this would be a very surprising conclusion.

---

[76] Cohen, *supra* note 75.

[77] *Id.*

[78] *See* FRANK PASQUALE, THE NEW LAWS OF ROBOTICS (forthcoming 2020) (manuscript at 75–77) (on file with the Harvard Law School Library).

[79] *See id.* at 180–82.

[80] *See* Jack M. Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIR. 45, 49 (2015).

[81] *See* Balkin, *Three Laws*, *supra* note 31, at 1223–25.

[82] Khan & Pozen, *supra* note 28, at 511–12; *see also, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 1, at 1227 ("Because personal data is a key source of wealth in the 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.").

[83] Khan & Pozen, *supra* note 28, at 512.

Instead, we should ask what practices of advertising, targeted at end users, do not betray their trust or operate against their interests. Only this kind of targeted advertising should be permitted.

Khan and Pozen speak of targeted advertising as if it were a single thing. It is not. And consequently, we do not face a simple choice of either having or not having targeted advertising. How targeted advertising works, the incentives it creates for companies, and its effects on end users are constructed by law as well as by technology.

Consider the distinction between contextual and behavioral advertising.[84] If I read a story on a website about Italy, I may be served ads about vacations to Italy as I move through the website. This is contextual advertising. The advertising is targeted at me because I visited the page or site, but it does not require the creation of an elaborate digital dossier about me to be effective. Behavioral advertising, by contrast, serves ads based on data collected about me in multiple settings. It may gather many kinds of data in order to make predictions about my interests and desires, and it may follow me in every application I use. A rule that allowed only contextual targeted advertising but not behavioral advertising would, at a stroke, transform the landscape of surveillance capitalism, but it would still allow targeted ads. And to the extent that advertising techniques evolve over time, such a rule could allow only techniques that are most like contextual advertising, requiring little in the way of persistent digital dossiers.

A total ban on behavioral advertising may not even be necessary. That is because behavioral advertising is not a single thing either. Like targeted advertising more generally, behavioral advertising refers to a range of different techniques made possible by both technology *and* legal rules. How companies engage in behavioral advertising depends on background legal restrictions on collection and use. Fiduciary obligations — and competition law! — can play a crucial role in structuring the legal background against which advertising occurs.

For example, if legal rules limit use, digital companies must develop advertising strategies that use the information they collect differently. If legal rules limit collection, companies must learn to adapt. For instance, they may spread their ads more broadly to reach more people instead of trying ever harder to influence a small number of people. Limiting data collection may also make it easier for other companies to compete with the current duopoly of Google and Facebook for advertising sales. This is an example of how fiduciary obligations can assist competition policy. But the assistance goes in both directions. If competition law limits

---

[84] *See generally* Betty Ho, *Targeting 101: Contextual vs. Behavioral Targeting*, CRITEO (Nov. 1, 2018), https://www.criteo.com/insights/contextual-vs-behavioral-targeting [https://perma.cc/H72J-9JZ2] (describing the distinction). Khan and Pozen tend to confuse the issue by treating targeted advertising and behavioral advertising as the same thing. *See* Khan & Pozen, *supra* note 28, at 511.

companies' accumulation of data, then companies' incentives change, and fiduciary obligations are less burdensome.

Moreover, it is still uncertain how effective many data-intensive behavioral strategies really are in promoting advertisers' businesses and increasing their sales. One of the deepest ironies of surveillance capitalism is that many of its practices may not actually benefit the advertisers they were developed for, while end users suffer the consequences. If companies must prove the efficacy of strategies to regulators, they may change their practices accordingly, benefiting both advertisers and end users.

We are still in the early stages of figuring out how digital advertisements actually work and the harms they actually cause. The more we learn about digital advertising, the more we may discover that some practices that initially seemed troublesome are mostly harmless, and those that seemed benign do real damage to end users and to the society in which they live. This is yet another reason to assign the task of concretizing fiduciary obligations to administrative agencies with appropriate expertise.

Above all, we should not take existing business models as given. If current advertising practices are abusive and predatory, the fiduciary model demands that companies change them. But that will still leave digital companies with many other advertising strategies from which they can still make plenty of money. After all, the fact that we outlaw fraud does not mean that nonfraudulent vendors cannot make a living.

V. THE FIRST AMENDMENT AND INTERMEDIARY IMMUNITY

A. Are Duties of Confidentiality Consistent with the First Amendment?

I have argued that the fiduciary model explains why many privacy regulations are consistent with the First Amendment.[85] Fiduciaries are normally subject to confidentiality rules and generally may not use or disclose information in ways that undermine the interests of their beneficiaries, clients, and patients. When fiduciaries disclose, distribute, or sell this information, the law treats them differently than it treats strangers who come across the same information, for example, newspapers and reporters.[86]

---

[85] *See, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 1, at 1209-20; Balkin, *Free Speech Is a Triangle*, *supra* note 1, at 2054; Balkin, *Algorithmic Society*, *supra* note 1, at 1161–62.

[86] *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 (AM. L. INST. 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*

The reason for this difference is that the disclosure occurs in the context of a confidential relationship of trust that the law regulates because of the client's vulnerability to abuse and manipulation.[87] As before, fiduciary obligations depend on underlying social relations. If Congress finds that end users are in a relationship of vulnerability to digital companies that requires fiduciary obligations, courts should treat the relationships between end users and these companies as relationships of trust, and protect end-user information in much the same way.[88]

To understand how the First Amendment interacts with privacy regulations, we must recognize that privacy regulations come in many different types. They can aim at several different stages in the flow of information. I like to categorize privacy regulations according to what I call the Great Chain of Privacy Being. They can be regulations concerning (1) collection of information, (2) collation, (3) analysis, (4) use, (5) disclosure and distribution, (6) sale, and (7) retention or destruction. This metaphorical chain of information flows does not cover all privacy regulations — for example, rules requiring the creation of a privacy bureaucracy or requirements of privacy by design — just the ones most likely to arise in a First Amendment context.

The First Amendment interacts differently with these different kinds of privacy regulations. Courts are more likely to treat restrictions on collection or use as not raising First Amendment questions at all, because they aim at conduct.[89] In the alternative, courts may treat them as content-neutral time, place, and manner regulations.[90] The most serious First Amendment problems usually arise on the "back end," when governments try to regulate disclosure, distribution, and sale of information. Here the First Amendment properly distinguishes between information obtained in the course of fiduciary relationships — which states can usually protect from disclosure — and information obtained in other contexts.[91] Under the same logic, governments may require confidentiality from information fiduciaries.

Khan and Pozen argue that the analogy to professional duties of confidentiality will prove unavailing.[92] They point to *National Institute of*

Disclosure of Paternity, 48 S.D. L. REV. 409, 413 & n.20 (2003) (collecting cases that hold that "a patient can recover damages for a breach of a physician's duty of confidentiality," *id.* at 413).

87 Balkin, *Information Fiduciaries*, *supra* note 1, at 1216–17.

88 *Id.* at 1218.

89 *See, e.g.*, Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1182–86, 1190–92 (2005) (noting the ubiquity of collection and use restrictions that do not violate the First Amendment).

90 *See* Bartnicki v. Vopper, 532 U.S. 514, 526 (2001) (explaining 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) (agreeing that restrictions on interception and disclosure were content neutral).

91 Balkin, *Information Fiduciaries*, *supra* note 1, at 1209–10, 1216–17.

92 Khan & Pozen, *supra* note 28, at 531–32.

Family & Life Advocates v. Becerra,[93] in which Justice Thomas stated that the Court has never "recognized 'professional speech' as a separate category of speech"[94] and that all content-based regulations of speech — presumably including professional speech — are subject to strict scrutiny.[95]

Becerra, however, did not actually involve a regulation of confidential speech in a professional relationship.[96] The Court did not suggest that doctor-patient confidentiality rules, restrictions on lawyers' disclosure of information about their clients, or a host of other standard limitations on professional speech are now subject to strict scrutiny. Indeed, Justice Thomas insisted that traditional regulations of professional conduct would remain untouched, "even though that conduct incidentally involves speech."[97] In other words, his statement in *Becerra* effectively treats all of the traditional restrictions on disclosure and use of client and patient information as regulations of "conduct," or else as content-neutral time, place, and manner regulations.[98] Whether or not this is a useful way of organizing First Amendment doctrine, it does not threaten these traditional professional restrictions on the use and disclosure of information.

Khan and Pozen's larger point, however, is that if the Roberts Court does not accept the analogy between digital businesses and other kinds of fiduciaries, the fiduciary model will not insulate privacy regulation from attack.[99] That is certainly true. But as Khan and Pozen admit, there is equally no guarantee that the Roberts Court will view their own novel theories about how to regulate platform companies as immune from First Amendment challenge.[100] The Roberts Court's current "weaponizing"[101] of the First Amendment in the interests of capital may defeat all of our reform efforts.

Instead we should focus on developing the best reading of the First Amendment. But if we want additional protection from an unsympathetic Court, there is yet another way to operationalize the fiduciary model.

---

[93] 138 S. Ct. 2361 (2018).

[94] *Id.* at 2371.

[95] *Id.* at 2371–72.

[96] *Id.* at 2373 ("The licensed notice at issue here is not an informed-consent requirement or any other regulation of professional conduct.").

[97] *Id.* at 2372.

[98] *See id.* at 2372–73; *see also* Bartnicki v. Vopper, 532 U.S. 514, 526 (2001); Richards, *supra* note 89, at 1188, 1190–94.

[99] Khan & Pozen, *supra* note 28, at 531–33.

[100] *See id.* at 533–34.

[101] Janus v. AFSCME, Council 31, 138 S.Ct. 2448, 2501 (2018) (Kagan, J., dissenting).

B. Public Interest Obligations for Social Media

Section 230 of the Telecommunications Act of 1996[102] gives companies that provide interactive computer services legal immunity from many lawsuits based on the content that other users provide.[103] Congress can require that if digital companies want the Section 230 immunity, they must agree to be regulated as information fiduciaries. (The condition could be limited to companies of a certain size or with a certain number of end users.) This immunity is important not only for social media and search-engine companies but also for all digital companies that allow end users and third parties to communicate, advertise, buy, and sell on their platforms. It is important to internet-of-things and robotics companies as well. All of these companies would have strong incentives to become information fiduciaries. And if companies refuse the deal, they still remain fully protected by the First Amendment.

The First Amendment does not require the full scope of Section 230 immunity — at least not as the courts currently construe it.[104] The First Amendment does prohibit the government from imposing strict liability on platforms for unlawful content appearing on the platform.[105] But Section 230 protects far more than this. Section 230 holds companies harmless for a wide variety of wrongs that occur on their platforms.[106] The difference in legal protection between what Section 230 offers and what the First Amendment requires is, in effect, a regulatory subsidy. Moreover, it is a particularly valuable subsidy.

In exchange for this subsidy, government should demand public interest obligations from digital platforms. These public interest obligations should combine competition policy, privacy, and consumer protection obligations.

First, as noted above, digital companies must accept that they are information fiduciaries toward their end users and toward any persons whose data they collect in the course of their businesses. This requirement means that if Facebook collects data about me from websites I visit and from my interactions with Facebook users, it agrees to be an

---

[102] 47 U.S.C. § 230.

[103] *Id.* § 230(c)(1).

[104] Eric Goldman, *Why Section 230 Is Better than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33, 36–44 (2019) (noting that Section 230's substantive and procedural protections extend well beyond the protections of the First Amendment). *But cf.* Note, *Section 230 as First Amendment Rule*, 131 HARV. L. REV. 2027 (2018) (arguing that courts should treat aspects of Section 230 as constitutionally required).

[105] *See* Smith v. California, 361 U.S. 147, 152–55 (1959) (holding that a bookstore could not be held liable for selling obscene books without knowledge of their content).

[106] Goldman, *supra* note 104, at 36–39 (noting substantive differences between Section 230 and First Amendment); *id.* at 39–44 (noting procedural benefits of Section 230).

information fiduciary toward me even if I do not have a Facebook account.[107]

Second, digital businesses must allow interoperability for other applications, as long as those applications also agree to act as information fiduciaries.

Third, digital businesses must allow government regulators to inspect their algorithms for purposes of enforcing competition law, privacy, and consumer protection obligations.

In a 2016 article, Professor Jonathan Zittrain and I proposed that the federal government could trade fiduciary obligations for federal preemption of state privacy laws.[108] The subsequent passage of the California Consumer Privacy Act[109] has altered the regulatory landscape.[110] In my view, it is better not to trade away states' abilities to protect end users, especially if one of those states is California, the home of Silicon Valley. Section 230 immunity is a far better bargaining tool.

So far Congress has altered Section 230 to require platforms to take down content that facilitates sex trafficking.[111] Other proposals require that platforms be "neutral" in their content moderation, an almost impossible demand.[112] Instead of focusing solely on content moderation, Congress should aim at deeper sources of digital power. It should ask digital companies to reshape their business models and reduce the incentives toward manipulation. Combined with competition law reforms, information-fiduciary obligations could go a long way toward changing the conditions of digital capitalism.

---

[107] *See* Daniel Kahn Gillmor, *Facebook Is Tracking Me Even Though I'm Not on Facebook*, ACLU (Apr. 5, 2018, 6:00 PM), https://www.aclu.org/blog/privacy-technology/internet-privacy/facebook-tracking-me-even-though-im-not-facebook [https://perma.cc/G7WL-SUDF].

[108] Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/4YR4-WAMC].

[109] CAL. CIV. CODE §§ 1798.100-.199 (West 2018).

[110] Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://nyti.ms/2lEdwdX [https://perma.cc/5YKC-3S2W].

[111] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018) (codified as amended in scattered sections of 18 and 47 U.S.C.).

[112] *See, e.g.*, Derek E. Bambauer, *How Section 230 Reform Endangers Internet Free Speech*, BROOKINGS INST.: TECHSTREAM (July 1, 2020), https://www.brookings.edu/techstream/how-section-230-reform-endangers-internet-free-speech [https://perma.cc/2V7H-XCWH].