Confiding in Con Men:
U.S. Privacy Law, the GDPR, and Information Fiduciaries

*Lindsey Barrett**

"We have a responsibility to protect your data, and if we can't then we don't deserve to serve you."

—Mark Zuckerberg, CEO of Facebook[1]

Zuck: *yea so if you ever need info about anyone at Harvard*
Zuck: *just ask*
Zuck: *i have over 4000 emails, pictures, addresses, sns*
Friend: *what!? how'd you manage that one?*
Zuck: *people just submitted it*
Zuck: *i don't know why*
Zuck: *they "trust me"*
Zuck: *dumb fucks*

—Id.[2]

ABSTRACT

In scope, ambition, and animating philosophy, U.S. privacy law and Europe's General Data Protection Regulation are almost diametric opposites. The GDPR's ambitious individual rights, significant prohibitions, substantive enforcement regime, and broad applicability contrast vividly with a scattershot U.S. regime that generally prioritizes facilitating commerce over protecting individuals, and which has created

* Teaching Fellow & Staff Attorney, Communications & Technology Clinic, Institute for Public Representation, Georgetown University Law Center. An enormous thank you to the participants at the *Seattle University Law Review* GDPR Symposium, the Yale Information Society Project, Jack Balkin, Joe Jerome, and Gabriela Zanfir-Fortuna for their enormously helpful comments, and another to the hard-working editors at the *Seattle University Law Review*.

1. Mark Zuckerberg, FACEBOOK (Mar. 21, 2018), https://www.facebook.com/zuck/posts/10104712037900071 [https://perma.cc/WD94-ZRH8].

2. Jose Antonio Vargas, *The Face of Facebook: Mark Zuckerberg Opens Up*, NEW YORKER (Sep. 20, 2010), https://www.newyorker.com/magazine/2010/09/20/the-face-of-facebook [https://perma.cc/R9ML-2XBZ].

perverse incentives for industry through anemic enforcement of the few meaningful limitations that do exist. A privacy law that characterizes data collectors as information fiduciaries could coalesce with the commercial focus of U.S. law, while emulating the GDPR's laudable normative objectives and fortifying U.S. consumer privacy law with a moral valence it often lacks. Similar to classic fiduciaries like doctors or lawyers, information fiduciaries would owe duties of loyalty, care, and confidentiality to their clients—affirmative commitments to individuals that the laissez-faire approach of U.S. privacy law generally does not require. Fiduciary duties are also derived from the context of commercial relationships, where the law balances the professional prerogatives of the fiduciary with the rights (and vulnerabilities) of the client. Crucially, an information fiduciary model can strengthen protections for privacy, equality, and autonomy in the digital age, echoing the GDPR's normative objectives, while balancing those principles with the competing aims (and constraints) of the U.S. legal ecosystem.

CONTENTS

INTRODUCTION

There is no longer any question that data collection can create privacy harms for individuals: the question is what the law can and should do about it. As various legal systems continue to produce a variety of answers, harmonizing the full gamut of approaches to privacy regulation in a globalized system is no small feat.

In the United States, consumer privacy law is shaped around a conception of privacy as a good, and is heavily motivated by the desire to foster an innovative climate for U.S. companies.[3] Data collection by private entities is governed by a patchwork of state and federal law that applies on a sectoral basis. If no sector-specific law applies—or the appropriate law excludes certain types of actors within the field, which is often the case[4]—the data collector is free to collect and use what it will, subject to the Federal Trade Commission (FTC) unfairness and deception enforcement authority.[5] The central goal of U.S. privacy law is to create an environment where industry experiments first and asks questions later, while privacy law that in any way hinders that ability is often criticized as paternalistic or retrogressive—or worse, European.[6]

---

3. Paul Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 132 (2017) (describing the "marketplace discourse" of privacy in the United States); *see, e.g.*, Roslyn Layton & Julian McLendon, *The GDPR: What It Really Does and How the U.S. Can Chart a Better Course*, 19 FEDERALIST SOC'Y REV. 234, 235–36 (2018) (describing the "serious and negative unintended consequences" of the GDPR and arguing that "[t]he American notion of privacy is predicated in large part on freedom from government intrusion and as a counterweight to the growth of the administrative state"); Maureen Olhausen, Acting Chairman, Fed. Trade Comm'n, Remarks at FTC Informational Injury Workshop 4 (Dec. 17, 2017), https://www.ftc.gov/system/files/documents/public_statements/1289343/mko_speech_-_info_injury_workshop_1.pdf [https://perma.cc/75JZ-4VP9] ("But if there are no harms, then data use restrictions impose only costs and no benefits.").

4. *See, e.g.*, 20 U.S.C. § 1232g (2012); 42 U.S.C. § 2000ff-5 (2012); 45 C.F.R. § 160 (2018).

5. This is true if the FTC has jurisdiction over the data collector, which is not always the case. The FTC does not have jurisdiction over common carriers, non-profits or other consumer areas where Congress has given oversight to another agency, such as the Federal Aviation Administration.

6. *See Charlemagne: Waiting for Goodot*, ECONOMIST (Oct. 13, 2018), https://www.economist.com/europe/2018/10/13/europes-history-explains-why-it-will-never-produce-a-google?frsc=dg%7Ce [https://perma.cc/JC2W-RTP2] ("Asked whether the continent will ever produce its own Google, one burst out laughing."); *see, e.g.*, *GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation: Hearing Before the S. Judiciary Comm.*, 116th Cong. 13 (2019) (statement of Rosalyn Layton, Visiting Scholar, American Enterprise Institute), https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony.pdf [https://perma.cc/HXX2-ALJM] (arguing, nine months after its implementation, that the GDPR has stymied innovation and the United States should "leapfrog" that regime with a more flexible approach); ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. INNOVATION FOUND., WHY STRONGER PRIVACY REGULATIONS DO NOT SPUR INCREASED INTERNET USE 2–3 (2018), http://www2.itif.org/2018-trust-privacy.pdf [https://perma.cc/6AB6-BRXN] ("Aggressive regulatory policies, such as those deployed in GDPR, will likely do little to nothing to increase trust, but will limit digital innovation and raise costs, thereby reducing use relative to more balanced rules. It is time, therefore, to end the spurious claims that more privacy regulation is pro-innovation and pro-consumer.").

In Europe, the conceptual and regulatory balance is reversed. As both privacy and data protection are considered fundamental human rights, legal protections for such rights are fulsome and tend to prioritize the protection of individual rights over ease of compliance for companies.[7] The EU's new General Data Protection Regulation (GDPR) reflects these normative commitments in aspects like the range of individual rights it creates, the breadth of its definitions and jurisdiction, the affirmative requirements and prohibitions it creates for industry, and the enforcement regime that ensures those objectives are actually met. The law has been globally influential, due to both the breadth of its applicability and the other laws it has inspired.[8] The ultimate impact of the GDPR's reach remains to be seen as regulators start to apply it and business practices start to shift, but U.S. state and federal lawmakers have already begun asking whether "GDPR-style" protections in the United States are possible, advisable, or even inevitable.[9]

As enthusiasm for new privacy regulation in the United States climbs, another approach to privacy regulation has been steadily gaining popularity: the idea of applying fiduciary duties like care, loyalty, and confidentiality to entities that collect digital information.[10] The idea of the information fiduciary, proposed by law professor Jack Balkin, takes an established legal relationship arising out of certain circumstances of trust, sensitive information exchange, and reliance, and applies it to the context of companies that collect, process, and store enormous amounts of digital information about individuals. Classic fiduciary relationships include doctors and patients, lawyers and their clients, or investment advisors and their clients.[11] These relationships are marked by the client trusting the fiduciary with sensitive information such that the fiduciary can provide a service that requires specialized skills or knowledge, and which the client cannot generally perform for herself. The resulting difficulty of supervision creates an incentive for the fiduciary to abuse the client's trust.

---

7. *See, e.g.*, William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 965–66 (contrasting the U.S. and EU approaches, as well as detailing the difference between data protection and privacy law); Schwartz & Peifer, *supra* note 3 (contrasting the U.S. and EU approaches).

8. Schwartz & Peifer, *supra* note 3, at 122 (calling the GDPR "stunningly influential" on privacy law around the globe).

9. Mark R. Warner, Potential Policy Proposals for Regulation of Social Media and Technology Firms 15–16 (draft white paper), https://graphics.axios.com/pdf/PlatformPolicyPaper.pdf [https://perma.cc/C9BR-8CB7]; *see also* Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html [https://perma.cc/QKQ4-2J2N].

10. Jack Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1152, 1162 (2018) [hereinafter Balkin, *Free Speech*].

11. *Id.* at 1162.

To prevent the fiduciaries from taking advantage of their clients, and to facilitate rational reliance on professionals who offer services that are universally needed but not universally capable of being performed, courts and legislatures have created fiduciary duties of care, confidentiality, and loyalty that forbid self-dealing and other abuses of this power dynamic.[12]

Balkin's proposal would extend similar duties to entities that hold themselves out as ensuring privacy to their users, or in situations where consumers of a service or product that collects data reasonably believed that their data would not be misused.[13] Jonathan Zittrain has similarly argued that given the ability of companies like Facebook to manipulate its users for opaque purposes, fiduciary duties could prevent data collectors[14] from self-dealing when their interests diverge from those of its users.[15] Doctors, lawyers, investment advisors, and other professionals are not permitted to act like "con men"[16] toward the people who reasonably trust them with their information. Balkin, Zittrain, and others argue that Uber, AirBnb, or Venmo should not be able to either.[17]

Applying duties of care, loyalty, and confidentiality to data collectors injects a moral valence to broadly uphold users' trust that U.S. privacy law generally does not require, and reverses the current presumption that data collectors generally bear no obligations to their users to a presumption that they do.[18] Under U.S. privacy law, a private actor that does not fall under the specific definition of a narrowly defined sectoral statute can largely do whatever it wants with the data it collects or otherwise obtains, provided it does not lie about its actions and attract the attention of an overstretched

12. Tamar Frankel, *Fiduciary Law*, 71 CALIF. L. REV. 795, 800 (1983).

13. Balkin, *Free Speech*, *supra* note 10, at 1162.

14. Except where a more specific term is warranted, I generally refer to the practices of "data collectors." This is to emphasize that while outsized harms may come from certain sectors and the incentives in need of remolding are primarily those of for-profit companies, the harms that a fiduciary framework would aim to prevent come from all corners of the digital ecosystem. Non-profits, universities, brick-and-mortar businesses and common carriers create many of the same types of issues that the digital platform companies do, and cannot be exempted from an effective fiduciary framework.

15. Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 340 (2014).

16. Jack Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/B7H2-BRHN].

17. *See id.*

18. Of course, U.S. privacy law already prohibits certain privacy-invasive practices. But the conception of privacy as a good, the focus on an easily navigated regulatory landscape, and the fact that the United States lacks a comprehensive privacy law have together created the understanding that to the extent that people accept an invasive practice, the government has no legitimate basis to prohibit it. Moreover, a rights-based approach assumes that the government has not only a basis but also an interest in ensuring that a threshold of protection exists. A duty of care is not as strong, but it creates the presumption of an obligation where one did not previously exist, while also adding a rights-like valence.

FTC.[19] In contrast, the GDPR places the onus on companies to justify their data collection and use, given its paramount objective of protecting individual rights—but that law relies on constitutional rights to privacy and data protection that are not present in U.S. law, and a different legal and historical understanding of privacy.

Classifying data collectors as information fiduciaries would not create an equivalent constitutional privacy right in the United States, like the one supporting the GDPR, but it would help correct the power imbalance between companies and individuals. Placing affirmative duties on data collectors deters exploitation of users, while a regime of "permissionless innovation" incentivizes it. Moreover, duties of care, loyalty, and confidentiality can be crafted and interpreted to forbid a broader array of digital harms that privacy law generally does not prevent, such as digital discrimination and manipulation. At the same time, an information fiduciary model may be more flexible and coalesce better with existing U.S. privacy law than the GDPR can, particularly as the fiduciary relationship arises in a commercial context and can accommodate the fiduciary's competing rights, professional objectives, and obligations that are also worthy of protection.[20] While U.S. privacy law often prioritizes companies over individuals and the GDPR is built upon constitutional rights against private entities that do not exist in U.S. law, an information fiduciary model can accommodate certain commercial objectives alongside a commitment to normative values such as privacy, autonomy, and equality that the law should uphold.[21]

This Article will begin with a brief background on the concept of information fiduciaries and traditional fiduciary law. It will then provide an overview of the stark asymmetry between companies and individuals in U.S. privacy law, including the marketplace focus of "consumer" privacy, the limits of U.S. privacy law to protect individuals from evolving digital harms, and weak enforcement. Part III will discuss the GDPR and its focus on the fundamental privacy rights of data subjects. Part IV will then describe how a fiduciary framework could coalesce with U.S. law while strengthening protections for individuals, even without an equivalent constitutional basis like the one undergirding the GDPR. Part V will address additional considerations.

---

19. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 470 (2016).

20. *See, e.g.*, Frankel, *supra* note 12, at 802 ("A fiduciary society attempts to maximize both the satisfaction of needs and the protection of freedom . . . . It permits the government to moderate between altruistic goals and individualistic, selfish desires, as well as between the social goal of increasing the common welfare and the individual desire to appropriate more than a 'fair share.'").

21. *Id.*

I. BACKGROUND ON INFORMATION FIDUCIARIES

As this Article will explain, the U.S. model of privacy regulation and the European model generally represent two extremes: "permissionless innovation" on one end and a strong commitment to individual rights on the other. Though divergent, the two approaches can still be mutually compatible in certain ways, and U.S. law would benefit from many of the legal innovations that the GDPR creates. State legislatures have already begun to emulate certain aspects of the GDPR, and some state constitutions already contain a right to privacy like the one undergirding the European law.[22]

But even if there were sufficient appetite from policymakers to incorporate the GDPR wholesale into federal law, the information fiduciary model coalesces better with the U.S. legal ecosystem than the GDPR can.[23] The concept of the fiduciary is deliberately designed to accommodate the needs and commercial prerogatives of the service provider, while recognizing that exploitation of the recipient's vulnerability is inevitable, undesirable, and legally preventable.[24] A fiduciary framework would not go so far as to create an equivalent constitutional right to privacy against private entities in the U.S., like the constitutional right that undergirds the GDPR. But affirmative duties based on the premise that individuals should be protected from digital exploitation can help correct the power imbalance between data subjects and data collectors, and transform how digital rights are understood.[25] Even without relying on a constitutional right to privacy, an information fiduciary framework would expand the kinds of harms that would be protected, while injecting a moral valence into a policy discussion that often lacks it. Finally, while this Article does not focus on the GDPR's incompatibility with U.S. law from a free expression standpoint, the fiduciary model is better equipped to accommodate the First Amendment in a way the GDPR is not.[26] Ultimately, the information fiduciary model

---

22. *See, e.g.*, CAL. CONST. art. I, § 1; ILL. CONST. art. I, § 6. Eleven states have constitutional rights to privacy. *Privacy Protections in State Constitutions*, NAT'L CONF. ST. LEGISLATURES (2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx [https://perma.cc/8JZB-KHZC].

23. *See, e.g.*, Tim Wu, *An American Alternative to Europe's Privacy Law*, N.Y. TIMES (May 30, 2018), https://www.nytimes.com/2018/05/30/opinion/europe-america-privacy-gdpr.html [https://perma.cc/NP8W-39LL].

24. *See generally* Frankel, *supra* note 12.

25. Compare with Frankel's argument that "[as] the entrustor should pay only for the benefits gained from the relation. . . . [F]air fiduciary law would shift the costs of protecting against abuse of power away from the entrustor to the fiduciary and the courts." *Id.* at 834.

26. JACK M. BALKIN, HOOVER INST., AEGIS SERIES PAPER NO. 1814, FIXING SOCIAL MEDIA'S GRAND BARGAIN 14 (2018), https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf [https://perma.cc/E5TW-G2XZ].

provides distinct advantages over the status quo of U.S. law that are inherent to the concept itself, but it also strikes a balance between the divergent approaches to privacy on each side of the Atlantic,[27] making it a fitting approach to U.S. privacy governance in a GDPR world.

While there is no sole definition of what constitutes a fiduciary or how the fiduciary relationship is created,[28] it generally arises when a person or entity relies on another with superior skills or knowledge for a service that they cannot easily perform themselves, based on the latter's expertise.[29] Providing a professional with sensitive information such that she can perform a service the client is unable to perform herself necessarily requires the fiduciary to have superior knowledge and makes her actions difficult for the client to effectively monitor.[30] The beneficiary must therefore trust that the fiduciary will accomplish the beneficiary's objectives as promised, which the law secures by placing duties of loyalty, care, and confidentiality on the fiduciary to prevent her from leveraging that dynamic to her advantage. Relationships in different contexts may give rise to different duties, but they typically include a duty of loyalty to the client, a duty of confidentiality, and a duty of care.[31] Classic examples of the fiduciary relationship include a doctor's duty to her patient, a lawyer to her client,[32] a union leader negotiating on behalf of workers,[33] or a trustee managing a trust on behalf of the trust's beneficiary.[34]

From a public policy standpoint, the state has an interest in protecting these relationships and ensuring that the client can rely on the fiduciary without fear that her information would be compromised. Violations could mean the suspension or forfeiture of a license to practice,[35] the cost of the

---

27. A rough analogy can be drawn with Frankel's description of classic fiduciary law: "[T]he moral feature of fiduciary law forms a bridge between altruism and individualism by focusing on the objectives towards which the fiduciary must aim." Frankel, *supra* note 12, at 832. Similarly, the information fiduciary model forms a bridge between the EU model's more idealistic focus on rights and the United States' focus on corporate growth.

28. New fiduciary relationships have been created over time, and a new one would not be unusual from the perspective of fiduciary law. *See id.* at 805.

29. *See* Balkin, *Free Speech*, *supra* note 10, at 1162 (discussing information fiduciaries); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 10 (2017) (defining fiduciaries); Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM. & MARY L. REV. 513, 519 (2015) ("Conventional fiduciary relationships are formed between fiduciaries and beneficiaries, and found an interpersonal form of accountability, realized through assignment of correlative rights and duties between the parties.").

30. Frankel, *supra* note 12, at 803–04 (describing how specialization and pooling enabled the development of the fiduciary relationship).

31. *See* Balkin, *Free Speech*, *supra* note 10, at 1161.

32. *Id.*

33. Frankel, *supra* note 12, at 795.

34. *Id.* at 805–06.

35. *See, e.g.*, MODEL RULES FOR LAWYER DISCIPLINARY ENF'T r. 10 (AM. BAR ASS'N 2017); FED'N OF STATE MED. BDS., U.S. MEDICAL REGULATOR TRENDS AND ACTIONS 2018, at 7 (2018),

disciplinary proceedings,[36] tort liability for malpractice,[37] or liability under other state laws.[38] The possibility of these kinds of punishment help to deter fiduciaries from exploiting power imbalances to their advantage. In addition to deterring violations by sanctioning errant fiduciaries, the law further reflects this normative tradeoff by limiting First Amendment protections for the fiduciary when she might otherwise wish to share the client's information[39] or providing an evidentiary shield when she might wish to avoid being legally compelled to divulge it.[40]

Ultimately, the relationship depends on trust: an expert seeking to perform services based on her superior knowledge needs to give potential clients a reason to trust her, and individuals seeking a service they themselves cannot perform must be able to trust the fiduciary on a more reliable basis than an irrational degree of good faith. The legal duties supplied by the fiduciary relationship enable this reliance. The fiduciary relationship is a commercial one—but with an unmistakably moral valence.[41]

II. U.S. PRIVACY LAW

The information fiduciary model is a vivid contrast to the status quo of U.S. privacy law. U.S. privacy protections are hobbled by U.S. privacy law's predominant objective of facilitating a robust environment for technological innovation and philosophically weakened by a conception of privacy as a good to be traded away, rather than a right to be protected. While the federal Constitution provides rights to privacy from the government, it does not provide the same protections for privacy from private entities, contributing to a diminished perception of the normative imperative of those protections in policy discussions.[42] In the seeming absence of a compelling basis to protect it, privacy from companies has come to be discussed as a commodity or a privilege that individuals should

---

https://www.fsmb.org/siteassets/advocacy/publications/us-medical-regulatory-trends-actions.pdf [https://perma.cc/D7GQ-LUT9].

36. *See generally* Neil Gordon, *Misconduct and Punishment: State Disciplinary Authorities Investigate Prosecutors Accused of Misconduct*, CTR. FOR PUB. INTEGRITY (Jan. 24, 2018), https://publicintegrity.org/accountability/misconduct-and-punishment/ [https://perma.cc/YMZ5-J9FW].

37. *See generally* Caroline Forell & Anna Sortun, *The Tort of Betrayal of Trust*, 42 U. MICH. J.L. REFORM 557 (2009) (detailing the tort regimes applicable to doctors and lawyers and arguing for a betrayal-based cause of action).

38. *See generally* Robert Kutcher, *Breach of Fiduciary Duties*, *in* BUSINESS TORTS LITIGATION 1 (Ann E. Georgehead et al. eds., 2d ed. 2005).

39. Balkin, *Free Speech*, *supra* note 10, at 1161.

40. *Id.* at 1161 n.30.

41. *See* BALKIN, *supra* note 26, at 11 (describing fiduciary law as "the law that governs the professions"); Frankel, *supra* note 12, at 830–32.

42. Schwartz & Peifer, *supra* note 3, at 133–34.

always have the prerogative to give up, while regulation that in any way inhibits their ability to do so is frequently decried as paternalistic and anti-innovation.[43] The conception of privacy as a good rather than a right is thus used to argue against strong consumer privacy protections that might hinder corporate success.[44] As the United States debates the merits of a possible comprehensive privacy law, this focus on regulatory flexibility for business is still heavily represented by the Trump Administration,[45] its

43. *See id.* at 119; *see also* McGeveran, *supra* note 7, at 975 (describing the "libertarian" approach to privacy taken by the U.S. Constitution); Richards & Hartzog, *supra* note 19, at 441 (critiquing the "harm fixation" in U.S. privacy law, arguing that "from this perspective, privacy is an injury to be remedied, a cost to be balanced in the ledger book, a harm rather than an opportunity" and noting that "critics of privacy regulation bemoan its toll on 'innovation' and 'progress'").

44. *See, e.g.*, Olhausen, *supra* note 3, at 4 ("But if there are no harms, then data use restrictions impose only costs and no benefits.").

45. Tony Romm, *The Trump Administration is Talking to Facebook and Google About Potential Rules for Online Privacy*, WASH. POST (July 27, 2018), https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/?utm_term=.0cd8f9076e05 (White House Deputy Press Secretary stating that "the Trump Administration aims to craft a consumer privacy protection policy that is the appropriate balance between privacy and prosperity . . . ."); *Senate Panel Opens Hearing on Crafting US Privacy Law*, VOICE OF AMERICA (Sept. 26, 2018), https://www.voanews.com/a/senate-panel-opens-hearing-on-crafting-us-privacy-law/4588164.html [https://perma.cc/D2TT-E9SK] (The same Deputy Press Secretary stating that the White House "look[ed] forward to working with Congress on a legislative solution" that strikes "the appropriate balance between privacy and prosperity . . . .").

agencies that work on privacy,[46] and the tech companies[47] and their surrogates.[48]

---

46. *See* Request for Comments, 83 Fed. Reg. 48,600–01 (Sept. 21, 2018), (describing the Trump's Administration's ideal approach to privacy as "a risk-management approach, one that affords organizations flexibility and innovation in how to achieve these outcomes"); Federal Trade Commission, Comment Letter on the National Telecommunications and Information Administration's Approach to Consumer Privacy 8–11 (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/federal_trade_commission_staff_comment_to_ntia_11.9.2018.pdf [https://perma.cc/C78C-QQJM] (noting that the FTC supports "a balanced approach to privacy that weighs the risks of data misuse with the benefits of data to innovation and competition," that "any approach to privacy must also consider how consumer data fuels innovation and competition," and emphasizing that privacy regulation should not unduly constrain innovation); Kang, *supra* note 9 (quoting David Redl, Assistant Secretary for Communications and Information at NTIA, that "commitment to prosperity will be our guide" on how privacy should be regulated); Olhausen, *supra* note 3, at 4; Ajit Pai, Chairman, Fed. Commc'n Comm'n, Remarks at the Newseum 1 (Dec. 12, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0427/DOC-344590A1.pdf [https://perma.cc/L2MN-CTL7] (calling the internet "the greatest free-market success story in history" in part due to the Telecommunications Acts' animating objective "to preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation").

47. While for years the tech companies have taken a more explicitly anti-regulatory posture, the current regulatory climate has produced a different strategy, namely a posture of cooperation and openness to regulation as a means to stave off more significant regulatory intervention. *See, e.g.*, Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—And Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [https://perma.cc/6S5V-27YX] (describing the tech companies' aggressive lobbying against CCPA, and how the Cambridge Analytica revelations "forced Facebook to take complaints about privacy more seriously—or, at least, to sound as if it did"); Sheera Frenkel et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html?rref=collection%2Fbyline%2Fcecilia-kang [https://perma.cc/VMS7-QVW6] (describing how Facebook "broke ranks with other tech companies, hoping the move would help repair relations on both sides of the aisle" in its support for SESTA/FOSTA); Cecilia Kang & Sheera Frenkel, *Facebook and Twitter Have a Message for Lawmakers: We're Trying*, N.Y. TIMES (Sept. 4, 2018), https://www.nytimes.com/2018/09/04/technology/facebook-and-twitter-have-a-message-for-lawmakers-were-trying.html?rref=collection%2Fbyline%2Fcecilia-kang [https://perma.cc/7U8U-FG2Q] (describing the "conciliatory and apologetic approach" Sheryl Sandberg and Jack Dorsey planned to take as they testified before Congress). Facebook has also presented a public face of being open to regulation while quietly lobbying against it behind closed doors, as have other tech companies. Kang, *supra* note 9 (describing aggressive lobbying Facebook, Google, IBM, and others for a "kinder set of rules" and how Facebook and Google "softened their resistance to a federal privacy law, as long as they were deeply involved in writing the rules"); Lee Fang, *Google and Facebook Are Quietly Fighting California's Privacy Rights Initiative, Emails Reveal*, INTERCEPT (June 26, 2018), https://theintercept.com/2018/06/26/google-and-facebook-are-quietly-fighting-californias-privacy-rights-initiative-emails-reveal/ [https://perma.cc/4SED-NQZ7] (describing how Facebook publicly supported CCPA while lobbying California lawmakers and donating money, along with Google, AT&T, Microsoft, Amazon, and Verizon, to defeat it).

48. *See, e.g.*, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274–75 (Dec. 2, 2016) (describing the Final Rule nullifying the FCC's broadband privacy rule as "designed to protect consumer choice while giving broadband providers the flexibility they need to continue to innovate"); Daniel Castro & Alan McQuinn, Info. Tech. & Innovation Found., Comment Letter on the National Telecommunications and Information Administration's Approach to Consumer Privacy 4 (Nov. 7, 2018), https://www.ntia.doc.gov/files/ntia/publications/2018-ntia-privacy-comments-itif.pdf [https://perma.cc/DFS6-ND3K] (arguing that a

The structural flaws of U.S. privacy law are exacerbated by the idea of privacy as a good. Without a more legally and conceptually fulsome *right* to privacy—rather than a right to trade it away—the basis for legal reforms seems weaker, and the arguments for the status quo are given more credence. The lack of a constitutional right to privacy from private entities has thus helped facilitate the construction of a consumer privacy regime primarily concerned with ease of compliance for companies, and shielded it from more consumer-protective modifications. The patchy protections of sectoral regulation, the failures of notice and choice without strong enforcement to compensate for them, and the narrow definitions of what kinds of harms merit judicial or administrative redress reflect this conceptual and legal diminishment of privacy, and often keep protections for it from being effective.

A. Sectoral Regulation

The fractal nature of privacy protections for individuals against private entities in the United States largely reflects a prioritization of corporate flexibility over individual rights. While an omnibus regime assumes that data collection should be justified, a sectoral regime assumes that any governmental *limits* on collection should be justified. As noted above, privacy from private entities is generally not protected by the U.S. Constitution.[49] Instead, an array of sector-specific state and federal statutes have established data collection and use limitations when legislatures determine a specific need for that particular industry, rather than by limitations on all data collection and use by default.[50] Statutes like HIPAA, FERPA, COPPA, GINA, GLBA and FCRA cover health information,[51] students' information,[52] children's online information,[53] genetic information,[54] and financial information[55] respectively.

---

federal privacy framework should "increase, not undermine, innovation," including by considering "the economic costs of any piece of privacy legislation or enforcement action," as "[o]verly strict data protection regulations can adversely impact innovation").

49. As McGeveran notes in *Friending the Privacy Regulator*, courts have inferred rights to privacy in discrete areas not explicit in the text, but "[t]his constitutional jurisprudence does not confer any broad right to control personal information equivalent to European human rights to data protection." McGevran, *supra* note 7, at 976; *see also* Schwartz & Peifer, *supra* note 3, at 133–34.

50. McGeveran, *supra* note 7, at 973–74 (describing the "smorgasbord" of privacy statutes that arose in response to "narrowly defined problems and [which] applies solely to the type of data connected with that problem"); *see also id.* at 977 ("Consumer protection law is tied to the inequitable nature of the underlying transaction, not to individual rights over personal data.").

51. *See, e.g.*, 45 C.F.R. § 160.102 (2018).

52. 20 U.S.C. § 1232g (2012 & Supp. V 2018).

53. 15 U.S.C. § 6501 (2012).

54. 42 U.S.C. § 2000ff–5 (2012).

55. 15 U.S.C. §§ 1681, 6801 (2012).

But even within the sectors that appear to be covered by pertinent statutes, narrow definitions cabin the applicability of such laws and the protections they appear to offer. For example, the Family Educational Rights and Privacy Act (FERPA), the statute governing collection of student data, applies to public school officials or those they designate.[56] It does not apply to any other entity that collects student data, such as a company that provides an official-looking survey as part of a test students are required to take, and then sells the information to data brokers.[57] Another example is the Genetic Information Nondiscrimination Act (GINA), the statute governing misuse of genetic data, which only prohibits the use in employment or insurance decisions.[58] While that is a good start, it does nothing to curb the behavior of consumer genetics companies, which are not otherwise subject to it, nor does it hamper any other use of genetic information other than in the insurance or employment contexts.[59]

As another example, the Health Insurance Portability and Accountability Act (HIPAA), which protects health privacy, only applies to information collected by a healthcare provider.[60] Any other collection or use of health information, for instance, by a healthcare startup selling predictive judgments on patients to insurance companies, or a period-tracking app hawking assessments of the likelihood that its users will conceive to their employers,[61] is not covered by the law.[62] Other sector-

56. 20 U.S.C. § 1232g (2012 & Supp. V 2018).

57. *See* Catherine Gewertz, *Students with Disabilities Sue ACT over Release of Personal Information*, EDUC. WEEK (Aug. 28, 2018), http://blogs.edweek.org/edweek/high_school_and_beyond/2018/08/students_with_disabilities_sue_act_over_release_of_personal_information.html [https://perma.cc/H88G-Y4JA] (describing a lawsuit brought by high school students alleging that the standardized testing company ACT collected and sold information about their learning disabilities to colleges. The suit rests on several federal and state laws, including the Americans with Disabilities Act and the California constitutional right to privacy, but not FERPA); Natasha Singer, *For Sale: Survey Data on Millions of High School Students*, N.Y. TIMES (July 29, 2018), https://www.nytimes.com/2018/07/29/business/for-sale-survey-data-on-millions-of-high-school-students.html [https://perma.cc/4666-X6BV] (describing how marketing programs collect and sell information about students, untrammeled by FERPA).

58. *See* Megan Molteni, *23andMe's Pharma Deals Have Been the Plan All Along*, WIRED (Aug. 3, 2018), https://www.wired.com/story/23andme-glaxosmithkline-pharma-deal/ [https://perma.cc/3S8U-KSYV].

59. *See, e.g.*, *id.*

60. 45 C.F.R. §§ 160, 162, 164 (2018).

61. Naomi Kresge, Ilya Khrennikov & David Ramli, *Period-Tracking Apps Are Monetizing Women's Extremely Personal Data*, BLOOMBERG: BUSINESSWEEK (Jan. 24, 2019), https://www.bloomberg.com/news/articles/2019-01-24/how-period-tracking-apps-are-monetizing-women-s-extremely-personal-data [https://perma.cc/8QN9-MS6G].

62. *See* Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, PROPUBLICA (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/X9B4-7G5Z]; Katie Thomas & Charles Ornstein, *Sloan Kettering's Cozy Deal with Start-Up Ignites a New Uproar*,

specific, definitionally limited federal privacy laws are the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), the two primary federal statutes that govern financial privacy. These two laws similarly rest on specific definitions of whom the law applies to and under what context it applies to them. GLBA applies to financial institutions (companies that offer consumers financial products or services like loans, financial or investment advice, or insurance) but ultimately provides fairly weak protections for consumers, as it simply requires covered entities to give consumers a right to opt out of having their information shared.[63] And while FCRA offers somewhat stronger protections, it only applies to consumer reporting agencies.[64] Thus, when an entity not fitting those descriptions—such as Facebook, Google, or a data broker—buys, sells, or shares financial information, such as credit card transactions, GLBA and FCRA do not apply. A sectoral approach means that entire areas are necessarily left open for exploitation due to reasons as unsatisfying as historical accident, industry pressure, or congressional inertia.[65] These narrowly defined laws also frequently fail to protect against new kinds of digital harms, such as manipulation or discrimination.[66]

The priorities of a sectoral approach are clear. This approach asks whether some new category of data *must* be regulated, because unless the harm occurring in the absence of regulation is particularly severe, the possible side effects of constraining industry practice should be considered more harmful to society than the invasions of privacy that intervention would seek to prevent.[67] In comparison, a comprehensive privacy law

---

N.Y. TIMES (Sept. 20, 2018), https://www.nytimes.com/2018/09/20/health/memorial-sloan-kettering-cancer-paige-ai.html [https://perma.cc/B42V-GEE6].

63. *See* 15 U.S.C. § 6801 (2012).

64. FED. TRADE COMM'N, A SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf [https://perma.cc/GLD9-586H].

65. *See, e.g.*, Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 360–61 (2015) (detailing the failures of various federal privacy bills, both comprehensive and sectoral); Alvaro M. Bedoya, *Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html [https://perma.cc/S8GT-W736].

66. *See, e.g.*, Allen, *supra* note 62 (noting that HIPPA does not limit the ability of insurance companies to surreptitiously use personal data purchased from data brokers to make medical assumptions that could lead to increased insurance prices); Adam Entous & Ronan Farrow, *Private Mossad for Hire*, NEW YORKER (Feb. 18, 2019), https://www.newyorker.com/magazine/2019/02/18/private-mossad-for-hire [https://perma.cc/83PT-SDC9] (describing the tactics of Israeli firms that specialize in digital manipulation campaigns, and discussing those firms' claims to legal legitimacy and the extent to which "regulations haven't kept pace with advances in technology").

67. Confessore, *supra* note 47 (describing the anger and frustration of privacy advocates with how industry pressure molded the Obama Administration's comprehensive privacy framework until it "retreat[ed] from the idea of consumer privacy as an inherent right," and that "[m]ost of the bill's protections applied only if collecting or using a given piece of information posed a serious risk of

starts with the premise that data practices *should* be prudently regulated to ensure the right to privacy is protected, rather than regulated as sparingly as possible.[68] The comprehensive approach assumes that privacy has a fundamental value for individuals, and the government should, as a part of maximizing any number of normative objectives for its constituents, ensure those protections. A sectoral approach prioritizes the ability of industry to move fast and break things, and subordinates strong privacy protections for individuals in favor of corporate flexibility to exploit them.[69]

B. The Failure of Notice & Choice

U.S. privacy laws also suffer from weaknesses that are not uniquely American, such as heavy reliance on notice and choice, a method of privacy regulation which promises transparency and agency but delivers neither. But while the GDPR still relies on notice and choice, it both recognizes its weaknesses and provides compensatory measures to account for them, such as requiring meaningful consent, prohibiting services from being contingent on coercive consent, assessing high fines for violations, and including transparency and access rights for individuals, as well as meaningful methods of administrative and judicial redress.[70] In contrast, U.S. privacy laws lack most of these compensatory measures, while still depending on the fiction that notice and choice provides individuals with control over their digital selves.[71]

---

economic or emotional harm"); Olhausen, *supra* note 3, at 4 ("Government does the most good with the fewest unintended side effects when it focuses on addressing actual or likely substantial consumer injury instead of expending resources to prevent trivial or purely hypothetical injuries. . . . [I]f there are no harms, then data use restrictions impose only costs and no benefits.").

68. McGeveran, *supra* note 7, at 966 (characterizing the "default rule" for privacy regulation as the most significant difference between the EU and U.S. regimes: "[I]n the United States, it is usually allowed unless the law says that it is not, while in the E.U. it is not allowed unless the law says that it is.").

69. *See, e.g.*, Oriana Senatore, U.S. Chamber Institute for Legal Reform, Comment Letter on FTC Informational Injury Workshop 3–4 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00023-141551.pdf [https://perma.cc/WF4T-LTAS] ("To fully achieve the maximum positive impact, organizations must be able to collect, share, and use information, subject to contractual limits and reasonable consumer protections to prevent fraud and deception, on the one hand, and without the threat of over-burdensome and disproportionate liability."); Brookman, *supra* note 65, at 361 (describing a House hearing on comprehensive privacy legislative "tellingly" titled "Internet Privacy: The Impact and Burden of EU Regulation" as part of the "death knell" that rang for the law as soon as President Obama endorsed it).

70. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 9(1), 2016 O.J. (L 119) 38 (EU) [hereinafter GDPR].

71. *See generally* James Cooper, Program on Economics & Privacy, Comment Letter on FTC Information Injury Workshop (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_

Fundamentally, "notice and choice" is a misnomer when few privacy notices offer sufficiently meaningful information capable of influencing the user's ultimate decision, and when a choice of whether to accept all the terms offered or simply seek a different product is often no choice at all.[72] Notice and choice has been roundly criticized by policymakers,[73] academics,[74] social scientists,[75] advocates,[76] and others[77] for quite some time, and with good reason. The idea that a generic description of a company's practices could possibly provide a sufficient disclaimer as to what data a company collects and how the data is used begs credulity; considering that the description is generally written in ten-point font and inscrutable legalese, is buried on the company's website, and is one of an unmanageable number that individuals encounter in a day, the proposition is laughable. People encounter so many privacy policies in their daily lives that it would be irrational to read each of them—one study calculated that it would take the average person 200 hours per year.[78] There are also all kinds of cognitive phenomena that prevent individuals from obtaining meaningful information from privacy policies in the way that a notice and

comments/2017/10/00019-141547.pdf [https://perma.cc/AN8M-VDG2] (arguing that the discrepancy between stated preferences and outcomes in privacy decision-making mediated by notice and choice should not compel strong privacy protections).

72. *See, e.g.*, Kashmir Hill, *Life Without the Tech Giants*, GIZMODO (Jan. 22, 2019), https://gizmodo.com/life-without-the-tech-giants-1830258056 [https://perma.cc/6VT5-P9FR] (documenting the veteran technology journalist's struggle, and occasional failure, to completely extricate Amazon, Facebook, Google, Microsoft, and Apple from her life).

73. Brian Fung, *'Your User Agreement Sucks': Mark Zuckerberg's Senate Grilling, in 10 Key Moments*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/your-user-agreement-sucks-mark-zuckerbergs-senate-grilling-in-10-key-moments/?utm_term=.e5b32914b30c [https://perma.cc/63MX-R9XE] (quoting Joe Kennedy criticizing Facebook's privacy policy by saying "your user agreement sucks").

74. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & POL'Y INFO. SOC'Y 543 (2008); *see, e.g.*, Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 952 n.1 (2017); Richards & Hartzog, *supra* note 19, at 444 (describing the failure of notice and choice and criticizing the "control illusion").

75. *See generally* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39 (2015); Florencia Marotta-Wurgler, Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies (Apr. 2015) (unpublished manuscript), https://www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf [https://perma.cc/KY8P-VUU5].

76. Electronic Privacy Information Center, Comment Letter on the National Telecommunications and Information Administration's Approach to Consumer Privacy (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/epic-ntia-nov2018.pdf [https://perma.cc/98Y3-STMJ].

77. Editorial, *How Silicon Valley Puts the 'Con' in Consent*, N.Y. TIMES (Feb. 2, 2019), https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html [https://perma.cc/2XF6-ETJH].

78. McDonald & Cranor, *supra* note 74, at 564.

choice regime assumes they do, such as hyperbolic discounting and optimism bias.[79]

In addition to the difficulty of locating privacy policies, interpreting them, and the other highly legitimate reasons that people have to not read privacy policies at all, many people do not understand their purpose. One survey found that 65% of respondents did not know that the statement "[w]hen a website has a privacy policy, it means the site will not share my information with other websites and companies without my permission" was incorrect.[80] Finally, "notice and choice" implies that a disclaimer regime requires companies to offer alternatives to practices the individual would prefer to prohibit. In reality, U.S. privacy policies are not required to offer alternatives that would enable the person to still use the product or service. It's not notice and choice, it's take it or leave it, and in most situations, "leaving it" is not a practical or even feasible option.

The end result of a notice and choice regime is a feasible mechanism for companies to demonstrate compliance, *not* a mechanism that prioritizes that people understand how their information is collected or used. The focus is on the procedure provided, not the outcome for the individual. A legal regime that relies on notice and choice can compensate for some of its weaknesses by providing additional rights for individuals, such as a private right of action to sue when their rights are violated, creating a higher threshold for what constitutes consent to a privacy policy, or strengthening accountability measures by empowering regulators with additional resources, enforcement powers, or expansive jurisdiction. The GDPR employs these kinds of mechanisms that are intended to compensate for the deficiencies of notice and choice. U.S. privacy law, for the most part, does not.

C. The Limits of FTC Enforcement

U.S. privacy protections are further hobbled by another practical limitation—the resources that are allocated for consumer privacy policymaking and the kind of enforcement authority regulators are permitted to wield. The Federal Trade Commission is the primary federal agency charged with protecting individuals from digital exploitation in a commercial context, including data privacy, security, and misuse by companies.[81] Its authority to police unfair and deceptive practices helps to

79. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1008 (2014) (describing the literature on cognitive biases that skew rational consumer behavior, such as optimism bias, information overload, anchoring, confirmation, and framing).

80. JOSEPH TURROW ET AL., THE TRADEOFF FALLACY 4 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [https://perma.cc/78ZC-FPL7].

81. State attorneys general also play an important role. *See generally* Danielle Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2017).

fill in some of the gaps left by the sectoral regime. For example, while only an employer or health insurance company's use of genetic information is subject to GINA, any company in the FTC's jurisdiction that used the information in a way that would constitute an unfair or deceptive trade practice would be subject to the FTC's oversight.[82] Ultimately, the agency's ability to police abusive privacy practices is severely curtailed by the limits of its statutory authority, its reactive rather than proactive approach to shaping privacy practices, and the sheer size of the job in comparison to the agency's available manpower, legal tools, and monetary resources.[83] Reticence to enforce also seems to play a role.[84]

As the sole backstop for the weaknesses of the rest of U.S. consumer privacy law, one agency can only do so much. To start, the FTC's authority does not include common carriers or non-profits, a limitation that some, like former Commissioner Terrell McSweeny and current Chairman Joe Simons, have argued should be lifted.[85] In an echo of how sectoral privacy laws leave broad swaths of conduct unregulated almost by happenstance, the FTC's lack of authority over common carriers leaves these entities free to violate people's privacy with near impunity. The agency also lacks general rulemaking authority, which means that its approach to shaping industry practice is primarily reactive, rather than proactive.[86] It polices industry practice on a case-by-case basis, in an approach that some have argued resembles how the common law builds on precedent and

82. As well as being subject to state privacy and Unfair and Deceptive Acts and Practices (UDAP) laws.

83. *See, e.g.*, Hal Singer, *The Latest Facebook Scandal Is Also a Crisis for the FTC*, SLATE (Dec. 19, 2018), https://slate.com/technology/2018/12/facebook-privacy-scandal-ftc-crisis.html [https://perma.cc/NXF9-P428].

84. Cecilia Kang & Nicholas Confessore, *Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites*, N.Y. TIMES (Dec. 30, 2018), https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html?rref=collection%2Fbyline%2Fcecilia-kang&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection [https://perma.cc/JP8D-D5RT].

85. Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence & Bots: Is The FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 529 (2018); *see also Oversight of the Federal Trade Commission: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 115th Cong. 4 (2018) (responses to written questions submitted to Joseph J. Simons, Chairman, Fed. Trade Comm'n), https://www.commerce.senate.gov/public/_cache/files/f15ec1e0-e736-44ce-912c-cb3c2dcdef10/1026963B4F5AA34FBDE922224104B601.majority-qfrs---joseph-j.-simons.pdf [https://perma.cc/97CJ-WB55] ("[T]he FTC could use broader enforcement authority to take action against common carriers and nonprofits."); McGeveran, *supra* note 7, at 977 (noting that the FTC's authorities do not extend to some financial institutions, telecommunications carriers, and airlines).

86. McSweeny, *supra* note 85, at 515 (describing the FTC as "the nation's primary consumer data protection agency").

establishes principles through the adjudication of individual controversies.[87]

Further, the FTC typically uses its deception authority in privacy and data security cases and rarely relies on its unfairness authority, with the latter requiring the agency to reach the lofty threshold of "a clear theory of substantial likelihood of harm to consumers that is not outweighed by any countervailing benefits."[88] The outsized role of deception in the FTC's policy means privacy abuses are limited to whether or not a company is forthright about its practices, regardless of whether the practice itself is inherently abusive, and to an often overly narrow view of what kind of injury constitutes a "material" harm.[89] As the vast majority of privacy policies are difficult to understand and rarely read, this reliance on deception leaves the FTC's enforcement as a fairly narrow sliver: an entirely truthful privacy policy is still a capable shield for practices that contravene consumer expectations or are otherwise exploitative.[90] Moreover, the agency's inability to level fines on the first instance of a company's malfeasance curtails its ability to deter such behavior.[91]

Even conduct that would appear to fit squarely within what the FTC would enforce can go unpunished, whether it is because of the agency's narrow definitions of informational harm, its limited enforcement authority, its lack of resources, or even institutional torpor.[92] While data

---

87. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 607 (2014).

88. McSweeny, *supra* note 85, at 522; *see also* G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 165 (2012) (describing the FTC's reticent approach to exercising its unfairness authority in privacy enforcement and arguing for a more aggressive approach).

89. Katie McInnis, Consumers Union, Comment Letter to the FTC Informational Injury Workshop 1–2 (Jan. 26, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00039-142816.pdf [https://perma.cc/3R8C-EU2C] (noting that "injury" is not an element in deception cases, and that "the Commission should not further hamstring itself in its mission to protect consumer interests"); Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361–63 (2014).

90. Google and Facebook, for example, both were reportedly tracking user location despite settings that would appear to indicate that tracking was not occurring. *See* Kashmir Hill, *Turning Off Facebook Location Tracking Doesn't Stop It from Tracking Your Location*, GIZMODO (Dec. 18, 2018), https://gizmodo.com/turning-off-facebook-location-tracking-doesnt-stop-it-f-1831149148 [https://perma.cc/ANC7-HR6A]; Ryan Nakashima, *Google Tracks Your Movements, Like It or Not*, AP NEWS (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb [https://perma.cc/B2CU-VRLG].

91. McSweeny, *supra* note 85, at 529 ("The FTC is capable of continuing to adapt to the digital age, but it must have the resources and tools to do so. As discussed above, Congress should grant the FTC rulemaking and civil penalty authority to protect consumers' privacy, security, and data rights.").

92. Singer, *supra* note 83 (criticizing the FTC's inertia on privacy enforcement and quoting former FTC official Justin Brookman that the "FTC could theoretically try to address [targeting users based on what they buy in the real world] under general Section 5 authority, *but they haven't tried* and it's unclear if they would be successful if they did") (emphasis in original).

breaches continue to rise in ubiquity and scale,[93] the action being taken to deter or prevent them is often unclear or unsatisfying, particularly as the FTC generally refuses to comment even on egregious cases.[94]

In a recent and notorious example, Facebook gave researchers affiliated with British political consulting firm Cambridge Analytica access to information on millions of its users without the users' consent, which Cambridge Analytica then used to attempt to persuade users to vote for its clients.[95] When Facebook found out what had happened, it hid that information from regulators, users, and the public.[96] This is an enormous abuse of its users' trust, and yet the question of whether the company would be punished by the FTC was initially somehow still uncertain,[97] despite the fact that the company was *already under a consent decree with the FTC for sharing user information with third parties without their consent*.[98] While it now seems likely that Facebook will face a large financial penalty for its misconduct, even a record-breaking fine may have limited deterrent or punitive value.[99] The largest privacy fine the FTC has ever assessed is $22.5 million, against Google;[100] Facebook's revenue for 2018 was nearly $56 *billion*,[101] making the likelihood of a fine that will

93. Mike Snider, *Your Data Was Probably Stolen in Cyberattack in 2018—And You Should Care*, USA TODAY (last updated Jan. 1, 2019), https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/ [https://perma.cc/H6PG-HYV8].

94. *See, e.g.*, Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests*, WASH. POST (Nov. 30, 2018), https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/?utm_term=.a6434b8a5dcf [https://perma.cc/9XDX-GRE5].

95. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

96. *Id.*

97. David C. Vladeck, *Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?*, HARV. L. REV.: BLOG (Apr. 4, 2018), https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/ [https://perma.cc/T9GT-FB4T] (arguing that the consent decree was violated); *FTC is Investigating Facebook over Cambridge Analytica's Use of Personal Data, Source Says*, L.A. TIMES (Mar. 20, 2018), https://www.latimes.com/business/technology/la-fi-tn-facebook-ftc-20180320-story.html [https://perma.cc/56H7-NKW4] ("Facebook said in a statement that it rejects 'any suggestion of violation of the consent decree.'").

98. Vladeck, *supra* note 97.

99. Tony Romm, *The U.S. Government and Facebook Are Negotiating a Record, Multibillion-dollar Fine for the Company's Privacy Lapses*, WASH. POST (Feb. 14, 2019), https://www.washingtonpost.com/technology/2019/02/14/us-government-facebook-are-negotiating-record-multi-billion-dollar-fine-companys-privacy-lapses/?utm_term=.82b5e2fdf4fb [https://perma.cc/KY33-F47U].

100. *Id.*

101. Press Release, Facebook, Facebook Reports Fourth Quarter and Full Year 2018 Results (Jan. 30, 2019), https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx [https://perma.cc/HJP9-83HK].

meaningfully change the company's approach decidedly slim.[102] As Chris Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius also note, no U.S. business has ever failed due to a regulatory fine imposed for privacy violations.[103]

The Commission has often emphasized its incremental and case-by-case approach as deliberately laissez-faire, underlining that the agency's goal is to foster innovation as much as it is to protect consumers.[104] But protecting consumers in a twenty-first century economy where ubiquitous commercial surveillance can both harm consumers and have anti-competitive effects requires an FTC that can prevent new kinds of informational harms, not simply react to them.[105] It requires an agency with enough resources and staff to fulfill its own mission while assisting other agencies that require its expertise to fulfill theirs.[106] Moreover, without significant curbs on their ability to abuse their market power, the largest tech companies lack a check on abusive data practices because people lack alternatives for the services they provide.[107] Limited

---

102. Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 65, 93 (2019); *cf.* David Steitfeld, *Big Tech May Look Troubled, but It's Just Getting Started*, N.Y. TIMES (Jan. 1, 2019), https://www.nytimes.com/2019/01/01/technology/big-tech-troubled-just-getting-started.html [https://perma.cc/546X-3WDY] (describing burgeoning growth among the tech giants despite backlash from consumers and regulators).

103. Hoofnagle et al., *supra* note 102, at 93; *cf.* Steitfeld, *supra* note 102.

104. Olhausen, *supra* note 3, at 3.

105. *See generall*y McSweeny, *supra* note 85.

106. Given the FTC's expertise in privacy, it collaborates fairly frequently with other agencies on public education and outreach, such as with the Department of Education, see, e.g., *Student Privacy and Ed Tech*, FED. TRADE COMM'N (Dec. 1, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech [https://perma.cc/4ECD-UMB8]; the National Highway Traffic & Safety Administration, see, e.g., Press Release, Fed. Comm. Comm'n, FTC, NHTSA Workshop to Focus on Privacy, Security Issues Related to Connected Cars (June 27, 2017), https://www.ftc.gov/news-events/press-releases/2017/06/ftc-nhtsa-workshop-focus-privacy-security-issues-related [https://perma.cc/88QW-AMG7]; the Department of Health and Human Services, see, e.g., Press Release, Fed. Comm. Comm'n, FTC Releases New Guidance for Developers of Mobile Health Apps (Apr. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps [https://perma.cc/LPN6-39F3]; and is frequently invoked as privacy guarantor by the FCC, see, e.g., Press Release, Fed. Comm. Comm'n, Statement of FCC Chairman Ajit Pai on Cogressional Resolution of Disapproval of FCC Broadband Privacy Regulations (Mar. 28, 2017), https://www.fcc.gov/document/chairman-pai-congressional-resolution-disapproving-privacy-regs [https://perma.cc/Z5XY-DU7D].

107. *See, e.g.*, Maurice Stucke, *Should We Be Concerned About Data-Opolies?*, 2 GEO. L. TECH. REV. 275, 321 (2018); *see also* David Cicilline & Terrell McSweeny, *Competition Is at the Heart of Facebook's Privacy Problem*, WIRED (Apr. 24, 2018), https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem/ [https://perma.cc/5TXZ-2ZQW]. FTC Commissioner Chopra has also argued for providing the agency with rulemaking power in order to bolster its competition enforcement authority. *See generally Competition and Consumer Protection in the 21st Century*: *Hearing Before the Fed. Trade Comm'n* (Sept. 6, 2018) (comment of Rohit Chopra, Commissioner, Fed Trade Comm'n), https://www.ftc.gov/system/files/documents/public_statements/1408196/chopra_-_comment_to_hearing_1_9-6-18.pdf [https://perma.cc/U4U7-HLTN].

competition in a market that rewards data collection and offers few liabilities for possible resulting harms means that companies have no incentive to improve the status quo.[108] As it stands, the agency charged with facilitating a competitive environment for innovation and protecting consumers from exploitation is often unable, and sometimes even unwilling,[109] to effectively do either.

D. Narrow Definition of Harm

A limited definition of what constitutes a privacy "harm" is also drawn from the idea of privacy as a good, rather than as a right, and further limits the ability of U.S. privacy law to offer comprehensive protections for individuals.[110] Under that theory, vigorous privacy enforcement does more harm than good because individuals should be able to trade away their information under nearly all circumstances, and companies should not be limited in their ability to coax them into doing so. A related corollary holds that informational injuries should be narrowly defined so as to include only the most egregious harms, such as physical injury or theft.[111] Limiting informational harms to physical or financial injuries allows more insidious injuries to individuals, such as reputational harms,

---

108. *See* Cicilline & McSweeny, *supra* note 107; *see also* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018) ("The value of personal data has led most companies to adopt a 'collect first, ask questions later' mentality. This mentality incentivizes design choices that marginalize users' interests in opacity and control over how their data is collected and used."); BALKIN, *supra* note 26, at 10.

109. Kang & Confessore, *supra* note 84.

110. Calo, *supra* note 89, at 363 (describing the narrow conception of privacy harms as an "(impossibly) high bar that some jurists and scholars expect privacy harm to overcome" and "suspicious").

111. *See* Ensuring Customer Premises Equip. Backup Power for Continuity of Commc'ns, 29 FCC Rcd. 14,968, 15,038 (2014) (Pai, Comm'r, concurring in part and dissenting in part) ("[W]e must act on concrete evidence, not hypothetical [privacy] harms."); Geoffrey Manne, Int'l Ctr. for Law & Econ., Remarks at the FTC Informational Injury Workshop (Dec. 12, 2017) (transcript available at pages 96–97 of *Informational Injury Workshop Transcript*, https://www.ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf [https:perma.cc/F6VN-YT5S]); Olhausen, *supra* note 3, at 4 ("Government does the most good with the fewest unintended side effects when it focuses on addressing actual or likely substantial consumer injury instead of expending resources to prevent trivial or purely hypothetical injuries."); Cooper, *supra* note 71, at 5 (urging a narrow and "precise" approach to informational injury); U.S. Chamber of Commerce, Comment Letter on The Informational Injury Workshop (Oct. 27, 2017), https://www.uschamber.com/sites/default/files/10.27.17_comments_to_ftc_on_informational_injury_workshop.pdf [https://perma.cc/4TP8-MNQW] ("The Commission should use this Workshop as an opportunity to adopt a regulatory framework that focuses on protecting consumers against concrete consumer harms as opposed to merely conjectural or hypothetical injuries."); The App Association, Comment Letter on The Informational Injury Workshop (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00024-141552.pdf [https://perma.cc/9TNZ-7R8J] (criticizing FTC investigations based on "hypothetical harms").

emotional harms, manipulation, or discrimination to persist. The FTC has also relied on a constrained definition of informational harms despite the fact that the bread-and-butter of its consumer privacy enforcement work, deceptive trade practices, do not require a showing of harm.[112]

While the FTC does acknowledge harms beyond the physical and financial,[113] its limited definition of privacy harms has curtailed its ability to protect consumers in the digital age, including by giving officials with a more pro-business bent a legalistic reason not to advocate more aggressively for consumers.[114] The judiciary has created additional barriers for individuals looking to vindicate their privacy rights by enforcing narrow readings of standing doctrine, such that plaintiffs struggle to bring privacy claims even in the rare cases where they are afforded the right to do so by statute.[115] The Supreme Court has ruled that violation of a statute does not constitute *per se* injury such that the plaintiff has standing to sue.[116]

An exhaustive list of the kinds of abuses that networked services enable and current U.S. privacy law does not forbid would fill a decent-sized encyclopedia, but a brief list of examples illustrates the range of ongoing harms. Facebook conducted a study on how to manipulate the mood of its users through its newsfeed without obtaining their consent or informing participants that it was happening.[117] A 2015 Carnegie Mellon study found that Google was more likely to target ads for high-income jobs to men than it was to women,[118] while a 2013 study found that Google

---

112. Calo, *supra* note 89, at 364.

113. Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 487 (2018) ("[N]arrow definitions of consumer injury that focus on traditional injuries, such as financial, health or safety harms, may not sufficiently account for intangible harms suffered by consumers as a result of 'privacy and data security missteps.'").

114. Kang & Confessore, *supra* note 84 ("Ms. Ohlhausen's staff told enforcement officials to slow down on cases, so the White House would not view her as anti-business, according to a former senior official. . . . With limited resources, she said, the F.T.C. should 'pursue cases where the evidence of actual or likely consumer harms is strongest.'").

115. *See* Brookman, *supra* note 65, at 365 (describing courts "narrowing the concept of Article III standing" as another avenue through which privacy protections in the United States are continuing to erode); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 748 (2016).

116. Spokeo v. Robins, 136 S. Ct. 1540 (2016); Richards & Hartzog, *supra* note 19, at 443 (noting state and federal courts' ever-narrowing approach to interpreting privacy harms).

117. *See* Gail Sullivan, *Sheryl Sandberg Not Sorry for Facebook Mood Manipulation Study*, WASH. POST (July 3, 2014), https://www.washingtonpost.com/news/morning-mix/wp/2014/07/03/sheryl-sandberg-not-sorry-for-facebook-mood-manipulation-study/?utm_term=.68197efa25ce [https://perma.cc/AWZ3-BQ7H]; David Gorski, *Did Facebook and PNAS Violate Human Research Protections in an Unethical Experiment?*, SCI.-BASED MED. (June 30, 2014), https://sciencebasedmedicine.org/did-facebook-and-pnas-violate-human-research-protections-in-an-unethical-experiment/ [https://perma.cc/5LHU-E3GJ].

118. Amit Datta et al., *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*, PROC. ON PRIVACY ENHANCING TECHS., Apr. 1, 2015, at 92.

searches for names common in the black community were much more likely to have target ads for arrest records databases.[119] Uber once threated to smear a journalist based on its knowledge of her whereabouts from using its app,[120] and the *New York Times* reported that Uber uses psychological tricks and gamification to get its drivers to work longer hours.[121] And a marketing company recently drew angry headlines for offering a consumer service that would attempt to influence women through targeted advertising to pursue sex with their husbands more frequently.[122]

While some of these harms might fall into what the FTC would consider deceptive conduct, or be forbidden under other laws, the agency's limited resources and narrow definition of harm make it highly unlikely that it would take enforcement action against these companies for the conduct described. Other misconduct—like Facebook failing to protect black users from being disproportionately targeted by Russian misinformation operations,[123] or Uber attempting to manipulate its contractors into working longer hours[124]—does not cleanly fit under the umbrella of a material harm due to deceptive conduct per the agency's definition at all, making it even less likely that an inert agency will investigate misconduct it sees as on the edge of its authority. Without regulators (or plaintiffs) to hold them accountable, companies continue to employ a range of techniques to wheedle their users into playing or scrolling longer, sharing more private information, or spending more

119. Latanya Sweeney, Discrimination in Online Ad Delivery 1 (Jan. 28, 2013) (unpublished manuscript) (on file with Harvard University, Data Privacy Lab), https://dataprivacylab.org/projects/onlineads/1071-1.pdf [https://perma.cc/NP46-SBGQ].

120. Jacob Kastrenakes, *Uber Executive Casually Threatens Journalist with Smear Campaign*, THE VERGE (Nov. 18, 2014), https://www.theverge.com/2014/11/18/7240215/uber-exec-casually-threatens-sarah-lacy-with-smear-campaign [https://perma.cc/49DW-6T6D].

121. Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers' Buttons*, N.Y. TIMES (Apr. 2, 2017), https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html [https://perma.cc/K8QF-VJNM].

122. Fiona Tapp, *New Service Promises to Manipulate Your Wife into Having Sex with You*, ROLLING STONE (Aug. 18, 2018), https://www.rollingstone.com/culture/culture-features/spinner-service-manipulate-wife-sex-712385/ [https://perma.cc/8MW8-L2GE].

123. RENEE DIRESTA ET AL., NEW KNOWLEDGE, THE TACTICS & TROPES OF THE INTERNET RESEARCH AGENCY 8 (2018), https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf [https://perma.cc/5SH9-MLNS].

124. Scheiber, *supra* note 121.

money,[125] while the design of their platforms frequently enables or outright incentivizes discrimination, harassment, or extremism.[126]

As this Section has briefly illustrated, the weaknesses of U.S. privacy law are heavily influenced by a policy approach that seeks to minimize the dangers of privacy violations, such that strong consumer protections are characterized as a barrier to innovation rather than a necessary safeguard. The laissez-faire approach to privacy regulation—and the prioritization of corporate flexibility over individual rights—is reflected on a macro scale in the choice of sectoral regulation over comprehensive privacy regulation, and on the micro scale with the default of most privacy laws allowing data collection—as opposed to a default requirement that data collection should be justified. The framing of privacy as a good that individuals should be able to trade away without limit, the narrow definition of digital harm, the inefficacy of notice and choice, and a legally and practically constrained FTC keep the law from sufficiently protecting individuals from evolving digital threats.

III. GDPR

The inspiration for the General Data Protection Regulation stands in clear contrast to that of U.S. privacy law: it is a framework that is primarily focused on the rights of the data subject and the imperative of protecting her, rather than on retroactively correcting whatever collateral damage results from facilitating the success of industries built on consumer surveillance.[127] The law is not a panacea for all digital harms and has been subject to critique on a range of issues.[128] But the philosophical and legal

125. *See* FORBRUKERRÅDET, DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS TO PRIVACY (2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [https://perma.cc/2YJS-EZFG]; Marisa Meyer et al., *Advertising in Young Children's Apps: A Content Analysis*, 40 J. DEV. BEHAV. PEDIATRICS 32 (2019); Henry Farrell, *It's No Accident that Facebook is so Addictive*, WASH. POST (Aug. 6, 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/08/06/its-no-accident-that-facebook-is-so-addictive/?noredirect=on&utm_term=.887db14b684e [https://perma.cc/5ZJA-5JM7].

126. *See* REBECCA LEWIS, DATA & SOCIETY, ALTERNATIVE INFLUENCE: DOCUMENTING THE REACTIONARY RIGHT ON YOUTUBE (2018), https://datasociety.net/wp-content/uploads/2018/09/DS_Alternative_Influence.pdf [https://perma.cc/GM9C-2KG6]; OLIVIER SYLVAIN, KNIGHT FIRST AMENDMENT INST., DISCRIMINATORY DESIGNS ON USER DATA (2018), https://knightcolumbia.org/sites/default/files/content/Sylvain_Emerging_Threats.pdf [https://perma.cc/Y3RJ-FGTJ].

127. *See, e.g.*, GDPR, *supra* note 70, Recital 1, at 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right.").

128. *See* Glyn Moody, *ICANN Loses Yet Again in Its Quixotic Quest to Obtain a Special Exemption from the EU's GDPR*, TECHDIRT (Aug. 8, 2018), https://www.techdirt.com/articles/20180808/03340740390/icann-loses-yet-again-quixotic-quest-to-obtain-special-exemption-eus-gdpr.shtml [https://perma.cc/N5M5-C7S3]; *Europe's History Explains Why It Will Never Produce a Google*, ECONOMIST (Oct. 13, 2018), https://www.economist.com/europe/2018/10/13/europes-history-explains-why-it-will-never-produce-a-google?frsc=dg%7Ce [https://perma.cc/EA9V-EJPB].

underpinnings of the GDPR's balance of competing interests are based on a fundamental, constitutional right to privacy and data protection that anchors the law in a commitment to individuals first and industry second, which does not exist in U.S. privacy law.[129]

A. Background on the Regulation

While the EU conception of privacy as a fundamental right arose before World War II, the atrocities to dignity and autonomy committed during the war created the impetus for the right to privacy to be formally codified in the Declaration of Human Rights,[130] the European Convention on Human Rights,[131] and the Charter of Fundamental Rights.[132] Following the creation of the European Union, the EU Data Protection Directive, a precursor to the GDPR, further created the legal framework for a streamlined digital single market in the EU with a recognition of the fundamental right to privacy created by the ECHR.[133] The EU Data Protection Directive relies on transposition to implement the goals of the Directive—the EU set the overarching objectives, but the member states can implement variations of the law's requirements, provided the domestic legislation meets minimum standards.[134] The Treaty of Lisbon made the right to privacy and the right to data protection constitutional rights binding on the member states.[135] The connection to human rights law gives privacy in the EU an additional measure of gravity that the U.S. framing of a "consumer's" data lacks.[136]

---

129. *See* Hoofnagle et al., *supra* note 102, at 70 (discussing the normative tradition of the GDPR and distinguishing the rights to data protection and privacy) ("Data protection focuses on whether data is used fairly and with due process while privacy preserves the Athenian ideal of private life."); *id.* at 72 ("The GDPR sets normative preferences in tension with information-intensive industry practices, particularly those performed by third parties.").

130. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

131. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

132. Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 10 [hereinafter EU Charter of Fundamental Rights] (Article 7 includes respect for private and family life, and Article 8 contains protections of personal data.).

133. Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *repealed by* GDPR, *supra* note 70, art. 94, at 86.

134. Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 617–18 (2013).

135. *See* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community art. 16B, Dec. 13, 2007, 2007 O.J. (C 306) 51; EU Charter of Fundamental Rights, *supra* note 132, arts. 7–8, at 10.

136. *See* Hoofnagle et al., *supra* note 102, at 66 (quoting one of the drafters of the Charter of Fundamental Rights of the EU, Stefano Rodota, describing the GDPR as a digital Magna Carta, with a corresponding online habeas corpus right, and noting, "These commitments germinated long before the rise of contemporary Silicon Valley data companies but have only intensified as such companies

The GDPR takes these commitments one step further. As a regulation, rather than a directive, its provisions are directly binding on member states, which, as Paul Schwartz and Karl-Nikolaus Peifer note in their insightful article comparing the EU and U.S. privacy regimes, reflects the primacy of the data subject in EU privacy law.[137] Both EU privacy law and the substance of the GDPR reflect this primary commitment to data subjects with a comparative disregard for industry prerogatives that would make a U.S. industry lobbyist blanch.[138] The preamble of the Regulation also makes this commitment clear.[139]

B. The GDPR's Protections for Privacy & Data Protection Rights

The GDPR is not entirely one-sided: it focuses both on the rights of individuals, and on simplifying the data protection regime for European businesses in a strengthened digital market. However, in both philosophy and substance, the law is primarily committed to the rights of individuals to control their information.[140] To start, the GDPR flips the presumption of U.S. privacy law—a data controller must have a legal basis to collect data, as opposed to collection being permitted unless it has been specifically prohibited.[141] The law's capacious definitions similarly reflect a default presumption of protection and a commitment to privacy as a right as opposed to a consumer good. Not only does U.S. privacy law distinguish privacy from private entities from privacy from the government in a way European law does not, the characterization of a "consumer" protection focuses on the subject's use of a good or service.[142] In contrast to the general characterization of a "consumer" right and the definition in many U.S. privacy statutes of subjects as "consumers" or

---

have gained dominance."); McGeveran, *supra* note 7, at 967 (describing the moral dimensions of EU data protection law); *id.* at 969 (describing the European legal conception of control of personal information as "a human right of the highest order"); Schwartz & Peifer, *supra* note 3, at 123–27 (describing the history and status of privacy and data protection law in the EU and noting "European data protection law is strongly anchored at the constitutional level. Its goal is to protect individuals from risks to personhood caused by the processing of personal data, and its favored mode of discourse is rights talk. When it discusses privacy, it uses the language of human rights to develop protections for its data subjects.").

137. Schwartz & Peifer, *supra* note 3, at 129.

138. *Id.* at 129–31 ("Free flow of information matters, but not as much, ultimately, as the safeguarding of dignity, privacy, and data protection in the European rights regime.").

139. GDPR, *supra* note 70, Recital 1, at 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right.").

140. *Id.* art. 1(2), at 32 ("This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.").

141. *Id.* art. 6, at 36.

142. *See* Schwartz & Peifer, *supra* note 3, at 132 nn.106–07 and accompanying text.

"subscribers," the GDPR generally applies to data subjects regardless of whether any kind of transaction has taken place, with a few exceptions.[143]

The GDPR prioritizes ensuring that data collection adheres to the subjects' expectations and that they have control over their information rather than focusing on how onerous establishing the basis for lawful processing may be.[144] Much has been made, for example, of the GDPR's requirements for obtaining consent, and how those might inhibit business practices.[145] The GDPR places a much higher bar for what constitutes consent, acknowledging that check-the-box clickwrap hardly ever constitutes meaningful decision-making. Controllers need consent for the "[p]rocessing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."[146] Consent must be freely given, specific and informed, subjects must be able to withdraw it, and receipt of a service must not be conditioned on providing it.[147] Preventing companies from relying on vague privacy policies which consumers must accept in order to use the product is a key part of giving individuals any kind of meaningful rights over their information, as well as an important element of correcting the inadequacies of notice and choice described above.[148]

The law also sets broad parameters for the definitions of key terms, such as what constitutes "personal data" and "processing." Personal data is "any information relating to an identified or identifiable natural person ('data subject')," while "an identifiable natural person" is defined as "one who can be identified . . . in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[149]

---

143. GDPR, *supra* note 70, art. 3(2), at 33 ("This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, *irrespective of whether a payment of the data subject is required*, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.") (emphasis added).

144. *See* Schwartz & Peifer, *supra* note 3, at 131 ("In this regime, economic interest in information and benefits on the 'supply side' regarding technology are not particularly important.").

145. *See, e.g.*, Sohin Gautam, *21st Century Problems: Will the European Union Data Reform Properly Balance Its Citizens' Business Interests and Privacy Rights?*, 21 SW. J. INT'L L. 195 (2014).

146. GDPR, *supra* note 70, art. 9(1), at 38.

147. *Id.* art. 7, at 37.

148. *See supra* Part I.

149. GDPR, *supra* note 70, art. 4(1), at 33.

"Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means."[150] The end result is that the majority of data is personal data, or is capable of becoming it, and nearly anything done with data is considered to be "processing," though the law exempts "purely personal or household activity" as well as national security.[151] In a similar reflection of how the definitions of the law are primarily concerned with the rights of individuals rather than the compliance obligations of businesses, requirements are not calibrated to the size of the business, as small businesses that handle sensitive data still have the potential to abuse it.[152] The GDPR's jurisdiction is similarly broad.[153]

The law further reflects a normative commitment to enshrining meaningful rights to privacy and data protection for individuals by codifying proactive access, correction, and objection rights. The GDPR gives individuals the right to know whether their information is being processed, to receive information about the processing, and to be provided with a copy of what has been processed.[154] Individuals also have a right to data portability and to rectify inaccuracies in the information controllers collect about them.[155] Other rights include the right to restrict processing, the right to object to processing taking place, and the right to erasure, also known as "the right to be forgotten."[156] The GDPR also recognizes the modern concerns of automated decision-making—fully automated profiling that can "produce legal effects or significantly affect" the subject is prohibited[157] unless there is a contract between subject and controller, and the processing is either authorized by law with suitable safeguard or based on the subject's consent.[158] Some of these rights are represented in U.S. law, many are not, and they are limited to the sector-specific statute

150. *Id.* art. 4(2), at 33.

151. *Id.* art. 2(2)(c), at 32; *see also* Hoofnagle et al., *supra* note 102, at 75.

152. Hoofnagle et al., *supra* note 102, at 73.

153. The GDPR applies to any entity that processes personal data "in the context of the activities of an establishment of a controller or a processor in the Union"—regardless of whether or not the processing occurs on EU soil—and to any entity that processes the data of EU subjects in order to offer them goods and services or to monitor their behavior. GDPR, *supra* note 70, art. 3(1)–(2), at 32–33.

154. *Id.* art. 15, at 43.

155. *Id.* art. 16, at 43; *id.* Recital 68, at 13.

156. *Id.* art. 17, at 43–44.

157. *Id.* art. 22(1), at 46; *see also* Hoofnagle et al., *supra* note 102, at 90 n.212 and accompanying texts (discussing scholarly interpretation of the relevant provision).

158. GDPR, *supra* note 70, art. 22(2), at 46.

rather than broadly applicable to nearly all processed information.[159] Others, like the right to data portability, are new.[160]

In addition to the substantive prohibitions and requirements the GDPR enacted to strengthen individual privacy rights, it also created a substantial enforcement regime to ensure its protections and prohibitions are a meaningful check on industry conduct. Violations of certain rules can trigger fines of up to 2% of global turnover, while more egregious violations can trigger fines of up to 4%.[161] The ability of individuals to receive judicial redress for violations also gives the GDPR teeth that U.S. privacy laws frequently lack, given that many U.S. privacy laws lack a private right of action. Even the laws that do have a private right of action still face a narrow approach to standing doctrine that often keeps privacy plaintiffs out of court, due to a limited definition of what constitutes "injury."[162] Under the GDPR, individuals can file complaints with Data Protection Authorities (DPAs), just as they can file them with the FTC in the United States, but the GDPR also provides an explicit right to an effective judicial remedy for data subjects, as well as creating a collective action mechanism.[163] Unlike the FTC, DPAs are also required to hear the complaints individuals file with them.[164]

Ultimately, the GDPR is a vast improvement on the Pollockian splattering of half-hearted statutes that protect privacy in the United States. It creates substantive rights to protect individuals from privacy invasions and the harms that can result from opaque automated processing. It also creates a significant enforcement regime to give those rights meaning and incentivizes compliance. But in addition to a basis in an almost diametrically opposed legal and political tradition,[165] the GDPR's commitment to individual privacy is supported by a comprehensive constitutional right to privacy and data protection that does not exist in U.S. law. An approach that bridges the gap between the U.S. laissez-faire approach to privacy regulation, and the prescriptive, rights-based European approach, can coalesce with the U.S. model while emulating the

159. COPPA, for example, affords parents the right to request that their children's data be deleted, and requires service providers to notify parents of that right. 16 C.F.R. § 312.4 (2018).

160. GDPR, *supra* note 80, Recital 68, at 13; *see also* Hoofnagle et al., *supra* note 102, at 89.

161. *Id.* art. 83(4)–(5), at 82–83.

162. *See* Hoofnagle et al., *supra* note 102, at 94.

163. GDPR, *supra* note 70, art. 80(1), at 81.

164. *Id.* art. 57(1)(f), at 68.

165. *See generally* Hoofnagle et al., *supra* note 102, at 72 ("[T]he GDPR has a dual goal of promoting the free flow of personal data within the EU (to help businesses), and protecting people and their personal data. Yet, the GDPR emphasizes the latter goal."); Schwartz & Peifer, *supra* note 3, at 131 ("Data protection law does not concern itself greatly with how its protection of the data subject might negatively impact useful activities of data processors.").

GDPR's commitment to individual rights—and perhaps even provide additional protections.

IV. APPLYING FIDUCIARY DUTIES TO DATA COLLECTORS

As this Article has attempted to illustrate, the philosophies and legal traditions behind the U.S. and European approaches to privacy regulation are distinct. The constitutional right to privacy and data protection in the EU places a high premium on how privacy is understood in policy discussions, and unsurprisingly, the GDPR is animated by an appropriately lofty commitment to meaningful protections for individuals that will actually be enforced. In contrast, the U.S. understanding of privacy as a good rather than a right minimizes the normative value of protections for it, while the increasingly narrow legal recourses for enforcing the few rights that do exist heavily limit their efficacy. Against this backdrop, an information fiduciary framework can strike the necessary balance of competing objectives: it is designed to balance commercial prerogatives with meaningful protections for individuals in the way that U.S. privacy law attempts, yet fails, to do. Moreover, the framing of data collectors owing affirmative duties to individuals injects a moral valence that the U.S. emphasis on privacy as a good otherwise eschews, as well as creating a presumption of obligations owed to individuals that does not currently exist.

Like traditional fiduciaries, companies that collect enormous amounts of data on individuals have a strategic advantage over their clients due to the fact that they are trusted with the user's sensitive information, in addition to superior and specialized knowledge, lack of transparency, and the reliance of their users on the specialized services provided.[166] Given a highly consolidated market and the low risk that enforcement poses to profitability, companies have every incentive in the world to

166. *See generally* Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law and Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 17–20 (2018) (describing the informational asymmetry between data collectors and the people relying on them for products and services, as well as the inability of individual users to understand or monitor their conduct due to structural challenges like lack of transparency); Lina Khan, *Sources of Tech Platform Power*, 2 GEO. L. TECH. REV. 325, 329 (2018) (discussing the power tech companies hold, including "information exploitation" of their users in discriminatory or privacy-invasive ways); Karen Levy & Solon Barocas, *Designing Against Discrimination in Online Markets*, 32 BERKELEY TECH. L.J. 1183, 1186 (2017) (discussing the power of networked platforms to deliberately discriminate or unintentionally facilitate discrimination against its users); K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1669 (2018) (describing the "unique kind of platform power" companies like Google, Facebook, Amazon, and Uber hold over the users, employees, and third parties that rely on their services).

leverage that asymmetry in their favor, and often do.[167] The ways that data collectors can take advantage of their subjects extends far beyond lying about data collection and use, and the harms extend beyond what privacy law generally protects, such as manipulation and discrimination.[168] Individuals deserve meaningful protections against violations of their privacy, and against the manipulation, exploitation, discrimination, and other harms that digital platforms are uniquely positioned to directly perpetrate or indirectly enable. A duty not to discriminate or manipulate also speaks to objectives similar to the GDPR's ban on fully automated decision-making based on profiling, given the risks to dignity and autonomy of reducing people to a series of opaque, and often biased, statistical evaluations.[169]

Crucially, applying fiduciary duties to data collectors would raise the bar of how digital companies are expected to treat their users' information. It would help adjust the objective of U.S. privacy law to more heavily prioritize the rights of the user, while still accounting for the commercial prerogatives of the collector. Fiduciary duties for doctors and lawyers have always recognized that legitimate professional objectives can coexist with the client's need for certain rights to be respected—a balance that can be wrought in the digital context as well. Duties of loyalty, care, and confidentiality can also prohibit digital harms such as manipulation, discrimination, and other harms that laws exclusively focused on privacy are ill-equipped to prevent, while still permitting non-harmful commercial activity.

The following Sections will describe what form an information fiduciary framework could take, and what it would need to incorporate in order to provide meaningful protections and change existing incentives for data collectors. They address why it is necessary for a fiduciary status to be compulsory, the importance of distinguishing between traditional and information fiduciaries, and what the duties of loyalty, care, and confidentiality could entail, including how those duties could expand the definitions of digital harm, and provide the basis for less trivial enforcement. Finally, they will address how an information fiduciary

---

167. *See* BALKIN, *supra* note 26, at 2–3 (noting the economic incentives of social media companies to promote engaging content "even if it is polarizing, false, or demagogic" and the capacity of bad actors to take advantage of that dynamic); *id.* at 4 (noting the economic incentives of social media companies to manipulate their users and to allow other to do it); Khan, *supra* note 166, at 325–28 (discussing the gatekeeper and leverage power of online platforms against their competitors).

168. *See* Richards & Hartzog, *supra* note 19, at 450–51 (describing how information disclosure creates vulnerabilities that data collectors can leverage in their benefit and to their users' detriment).

169. INFO. COMM'R'S OFFICE, GUIDE TO THE GENERAL DATA PROTECTING REGULATION 149 (Aug. 2018), https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf [https://perma.cc/9YWJ-YZJZ].

framework should approach both direct harms and negligent ones enabled by the design of the platform, or through lax enforcement of its policies.

A. Distinguishing Traditional Fiduciaries

As Balkin and Zittrain have noted, fiduciary duties for data collectors must be tailored to the context they are being created for, and both have argued that the expectations of good faith and fair dealing for information fiduciaries should be lower than what is expected of traditional fiduciaries.[170] Traditional fiduciaries are generally prohibited from benefitting from their clients' information in a way that could hurt the client: using client information to enrich themselves in a way that disadvantages the client would violate the duty of loyalty, and sharing it beyond prescribed limits would violate the duty of confidentiality.[171] Yet for certain business models, like social media companies or data brokers, profiting from their users' information seems like the very foundation of the product data collectors provide. Certainly, any application of fiduciary duties to data collectors would need to distinguish the kinds of conduct that are inherent to the service—such as a search engine "discriminating" by sorting through information and only providing the responsive results—from disloyal conduct designed to benefit the data collector to the detriment of the subject.[172] And as with traditional fiduciaries, the extent of the duty should also correspond to the degree of power imbalance, as Neil Richards and Woodrow Hartzog argue, as should the severity of the punishment for violating it.[173]

Granted, the degree of trust that users place in a cloud service or a social media platform is often different from the trust they place in a doctor or a lawyer, as the services and vulnerabilities are different.[174] But the information such a company holds can be no less sensitive by virtue of seeming more banal. Providing your location so that an Uber can take you to a bar is a transaction of much more limited scope and gravity than telling your lawyer incriminating details she intends to use for your defense. The balance shifts when you take an Uber to a more sensitive location, such as a protest site, an abortion clinic, or a temple, or when the information is used in aggregate to piece together your movements over a period of time,

---

170. Balkin, *Free Speech*, *supra* note 10, at 1162; *see also* Balkin & Zittrain, *supra* note 16.

171. *See* BALKIN, *supra* note 26, at 15.

172. *See* Richards & Hartzog, *supra* note 19, at 470 (distinguishing the relationship of a data collector and subject from a traditional fiduciary and the client).

173. *Id.* at 458; Frankel, *supra* note 12, at 825.

174. Frankel, *supra* note 12, at 825 ("These rules vary with the extent of the entrustor's vulnerability to abuse."); *id.* at 832 ("[T]he degree of moral culpability of the fiduciary is positively related to the extent of the entrustor's helplessness.").

or to be turned over to law enforcement.[175] The balance is shifted even further after considering that any information that Uber stores could be used by the company to enrich itself at your expense or to shut out competitors, be breached by a hacker, accessed by law enforcement, or used to blackmail you.

A key distinction between the expectations attached to traditional fiduciaries and how data collectors have been permitted to function is the presumption of an obligation of good faith and fair dealing in the absence of specific proscriptions.[176] There is a space between the loyalty and good faith one reasonably expects from a doctor or lawyer, and what one expects from the various companies that provide digital products and services. But that space exists because of the legal vacuum that has allowed data collectors to invade, exploit, and manipulate with impunity, not because the vulnerability of their users will always be smaller than that of a doctor's patients, or because a lawyer's ability to abuse her power over her clients is always greater than the power tech platforms wield over their users. Information fiduciary duties must be created with an eye for context, but not the flat assumption that the power dynamic between an individual and an online banking provider, an ISP, a picture storage service, a dating platform, or any other digital intermediary lacks the kind of moral valence that classic fiduciary relationships have been deemed to have, or the same potential for abuse of power.

It is also worth emphasizing that while the contexts in which different professions have developed fiduciary principles are distinct, that does not render a fiduciary approach inapposite for data collectors. The principles behind conflicts of interest rules in medicine or law are not so morally lofty and restrictive that they are inherently inapplicable to the context of data collectors—quite the opposite.[177] The ethical codes governing doctors and lawyers both provide leeway for conduct that does not entirely subordinate the fiduciary's interest to the client's when the two conflict.[178]

---

175. *See generally* RACHEL LEVINSON-WALDERMAN, BRENNAN CTR. FOR JUSTICE, CELLPHONES, LAW ENFORCEMENT, AND THE RIGHT TO PRIVACY 2–3 (2018), https://www.brennancenter.org/sites/default/files/publications/2018_12_CellSurveillanceV3.pdf [https://perma.cc/HJD6-UMLG] (discussing the collection of cellphone location data and law enforcement use of it); Tonya Riley, *Civil Rights Groups Aren't Impressed by Facebook's Efforts to Fight Discrimination*, MOTHER JONES (Dec. 18, 2018), https://www.motherjones.com/politics/2018/12/facebook-civil-rights-audit-color-of-change-russian-disinformation-african-americans/ [https://perma.cc/6X7P-ZUGM].

176. Balkin, *Free Speech*, *supra* note 10, at 1162.

177. *See generally* Forell & Sortun, *supra* note 37 (criticizing the insufficiency of existing methods of regulating the conduct of doctors and lawyers and arguing for a tort based on betrayal by fiduciaries in those professions).

178. A striking example of this is the medical tradition of allowing medical students to perform pelvic exams on unconscious female patients for the sake of the students' education, when the patients have not been informed that the exam would take place. Phoebe Friesen, *Why Are Pelvic Exams on Unconscious, Unconsenting Women Still Part of Medical Training?*, SLATE (Oct. 30, 2018), https://

In their thorough and thoughtful critique of the information fiduciary model, Lina Khan and David Pozen argue that any business model that relies on behavioral advertising is antithetical with a requirement that the fiduciary place the client's interests above her own, underlining the point with a hypothetical "Dr. Marta Zuckerberg" who derives her income from "enabling third parties to market [her patients] goods and services."[179] Yet the pharmaceutical industry's influence on prescribing practices make this hypothetical very real, as do the conflicting incentives of doctors with a financial stake in the medical devices they recommend.[180] One need not imagine a hypothetical Dr. Zuckerberg who derives income from recommending products to patients when lawsuits and reporting have clearly demonstrated the role that Purdue Pharma's sales tactics have played in creating the opioid crisis.[181] The ethical rules governing conflicts of interest for lawyers are also far from iron-clad. Lawyers are prohibited from using their client's information to disadvantage the client—but may do so if the client provides informed consent.[182] There is certainly a range of critiques that can be leveled against how existing fiduciary rules accommodate conflicted conduct, but these fields are hardly strangers to the kind of inherent conflicts implicated by data collection.[183] Fiduciary rules are flexible to professional prerogatives, but they are not toothless, and they implicate a moral dimension to the regulation of commercial conduct that other consumer protection regulation does not automatically

---

slate.com/technology/2018/10/pelvic-exams-unconscious-women-medical-training-consent.html [https://perma.cc/L4WT-QGS3] (citing Stephanie Schniederjan & G. Kevin Donovan, *Ethics Versus Education: Pelvic Exams on Anesthetized Women*, 98 J. OKLA. ST. MED. ASS'N 386 (2005)).

179. Lina Khan & David Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. (forthcoming 2019) (manuscript at 13) (on file with Harvard Law Review).

180. Forell & Sortun, *supra* note 37, at 559 (describing the conflicts of interest created by the pharmaceutical industry and the lack of legal ramifications); Nancy J. Moore, *What Doctors Can Learn from Lawyers About Conflicts of Interest*, 81 B.U. L. REV. 445, 455 (2001) (discussing the conflict of interest in doctors receiving monetary incentives for enrolling their patients in clinical trials).

181. Michael Forsythe & Walt Bogdanich, *McKinsey Advised Purdue Pharma How to 'Turbocharge' Opiod Sales, Lawsuit Says*, N.Y. TIMES (Feb. 1, 2019), https://www.nytimes.com/2019/02/01/business/purdue-pharma-mckinsey-oxycontin-opiods.html [https://perma.cc/9PKV-QMAR] ("McKinsey also recommended that Purdue redirect its sales force to focus on doctors who were especially prolific prescribers of OxyContin, according to the suit. One slide made public by the attorney general's office, attributed to McKinsey, focused on one doctor in the town of Wareham, Mass., who almost doubled his annual output of OxyContin prescriptions after a big increase in visits from Purdue sales representatives."); Barry Meier, *Sacklers Directed Efforts to Mislead Public About OxyContin, Court Filing Claims*, N.Y. TIMES (Jan. 15, 2019), https://www.nytimes.com/2019/01/15/health/sacklers-purdue-oxycontin-opioids.html [https://perma.cc/C2FB-MLMJ] (describing the Massachusetts lawsuit claiming that Purdue "aggressively" promoted the drug to doctors who were big opioid prescribers).

182. MODEL RULES OF PROF'L RESPONSIBILITY r. 1.8 cmt. 5 (AM. BAR ASS'N 2018).

183. *Contra* Khan & Pozen, *supra* note 179, at 13.

invoke, and which much of the U.S. discourse around privacy as a good attempts to repudiate.

Ultimately, the fact that the business models of many tech companies seem to be predicated on exploitation of their users simply demonstrates the aspects of those businesses that an information fiduciary framework would prohibit, not that an information fiduciary framework is logically incoherent. Exploitation of users' information should not be required for digital products and services to function, and for most of them, it is not. A social network need not be inherently manipulative, discriminatory, or privacy-invasive—the same is true for an internet service provider, a rideshare company, a medical device company, or a cloud service. A media company can rely on subscriptions;[184] a search engine can rely on contextual advertising.[185] To the extent that behavioral advertising or renting out user information to third parties undermines a duty of loyalty, that does not mean that a fiduciary model cannot be applied to data collectors; it means that exploitative practices will be prohibited, and non-exploitative services and products will not be.

B. Compulsory Fiduciary Duties

In order to be effective, any attempt to characterize data collectors as information fiduciaries must be compulsory rather than optional. Both Balkin and Zittrain suggest that a fiduciary framework could be opt-in, with a law that would preempt state privacy laws for the companies that choose to join.[186] This approach would certainly bolster the political feasibility of any fiduciary proposal, and the looming deadline of a new privacy law in California has made tech companies claim to be more amenable towards a new comprehensive, federal privacy law than they

184. Jenny Luna, *Why Every Business Will Soon Be a Subscription Business*, STAN. BUS.: INSIGHTS (Aug. 17, 2018), https://www.gsb.stanford.edu/insights/why-every-business-will-soon-be-subscription-business [https://perma.cc/QX88-EDC6] (describing the rise of subscription-based business models).

185. Natasha Lomas, *The Case Against Behavioral Advertising Is Stacking Up*, TECHCRUNCH (Jan. 24, 2019), https://techcrunch.com/2019/01/20/dont-be-creepy/ [https://perma.cc/UF56-J9MW] (describing the success of DuckDuckGo, which relies on search-based ads rather than behavioral advertising based on the information it collects from its users); *see also* Jessica Davies, *After GDPR, The* New York Times *Cut Off Ad Exchanges in Europe—And Kept Growing Ad Revenue*, DIGIDAY (Jan. 16, 2019), https://digiday.com/media/new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/ [https://perma.cc/W6WP-8S5E] (describing how the *New York Times* switched to contextual advertising from behavioral advertising in order to comply with the GDPR and saw its advertising revenues rise).

186. BALKIN, *supra* note 26, at 15; Balkin & Zittrain, *supra* note 16; Zittrain, *supra* note 15, at 340.

have been in the past.[187] But a voluntary regime shaped by the lobbyists for the companies it would purport to regulate will be subject to the same broad provisions and tepid commitments of other self-regulatory programs that have been largely ineffective.[188] The result is a catch-22—either the new federal law is too weak to be impactful in order to coax companies to join the safe harbor, or the law creates meaningful protections and enforcement, and the companies have no reason to join.[189]

While an opt-in regime seems temptingly seamless, I share the skepticism that Lina Kahn and David Pozen express in their appropriately titled essay that it could produce the kind of meaningful change the digital ecosystem so desperately needs.[190] Rather than a significant realignment in incentives and philosophy, the result will be additional lip service by some companies to privacy (and ammunition against further enforcement or regulation), no change from others, and little impact on the status quo for individuals.[191] The U.S. privacy landscape is far too skewed towards corporate priorities for a program industry-friendly enough to tempt voluntary compliance to be capable of restoring the equilibrium. For a fiduciary framework to have real force, it must apply compulsory duties for information fiduciaries, and provide for real enforcement when those duties are violated.

---

187. Kang, *supra* note 9 (describing the lobbying efforts of Facebook, IBM, Microsoft and other companies to cajole Congress into preempting state privacy laws for a gentler federal one in the wake of CCPA's passage); *see also* sources cited *supra* note 47.

188. *See, e.g.*, Frankel, *supra* note 12, at 816 (arguing that self-regulatory organizations incentivize members to "minimiz[e] the burdens of self-regulation" and is an incomplete solution to the problems the fiduciary relationship would seek to solve).

189. *See, e.g.*, Margot Kaminski, *When the Default Is No Penalty: Negotiating Privacy at the NTIA*, 93 DEN. L. REV. 925, 946 ("Coupled with evidence from the NTIA negotiations thus far, this suggests that both the current penalties and the current levels and kinds of uncertainty in the U.S. privacy regime are not enough to drive industry to the table in efficiency-maximizing ways.").

190. Khan & Pozen, *supra* note 179, at 29–30. I do, however, respectfully disagree with the authors that a fiduciary approach precludes the kinds of structural reforms that they argue, and I full-heartedly agree, are needed, provided the fiduciary characterization is mandatory, and the framework includes additional mechanisms to change the incentives around data abuses. These incentives include rulemaking and civil penalty authority for the FTC (or broad authority and considerable resources for a new data protection agency), access to the courts through a private right of action for individuals, an expanded definition of digital injury, and other reforms that Balkin and Zittrain's framework either does not specifically address or excludes.

191. *See* Frankel, *supra* note 12, at 816 (noting the limits of self-regulatory organizations in preventing abuse of power by fiduciaries, given that "[i]ts members may be interested in minimizing the burdens of self-regulation and maximizing the benefits of the organization's monopoly"); *id.* at 832 ("[T]he degree of moral culpability of the fiduciary is positively related to the extent of the entrustor's helplessness."). Privacy policy is certainly no stranger to the failures of self-regulation. *See generally* Brookman, *supra* note 65, at 362–63 (The cycle of "once interest in legislation perks up on Capitol Hill, industry scrambles to demonstrate its own capacity to address the problem itself. Once Congress's attention has waned or turned to other matters, however, industry momentum toward meaningful rules often falls by the wayside" has repeatedly failed in the privacy space.).

C. Information Fiduciary Duties: Loyalty, Care, Confidentiality

Generally, any information fiduciary framework should require duties of loyalty, care, and confidentiality, though there is a range of what specific obligations those duties could entail. Balkin argues for duties of care, loyalty, and confidentiality,[192] characterizing the primary obligation of the information fiduciaries as not acting like a "con artist" by inducing trust in their users to obtain their information, then using that information to the benefit of the fiduciary and the detriment of the user, in violation of that trust.[193] As an example, fiduciaries should be prohibited from "hold[ing] themselves out as providing digital safety and respecting digital privacy and then manipulat[ing] and discriminat[ing] against their end-users," and prohibited from sharing or selling data from or about their users to entities not subject to its fiduciary duties.[194] Zittrain focuses on the political dimensions of manipulation, stating that "a central responsibility of an information intermediary would be to serve up others' data in ways not designed to further the political goals of the intermediary."[195] The Data Care Act, a comprehensive legislative framework recently proposed by Senator Brian Schatz and fourteen other senators, sketches out broad duties of loyalty, care, and confidentiality, while providing the FTC with rulemaking authority to determine the details.[196] In a relevant and cogent article advocating for the role of trust in privacy law, Neil Richards and Woodrow Hartzog discuss the value of incorporating duties of loyalty, confidentiality, and care into privacy law, though they do not argue for a scheme of compulsory fiduciary duties *per se*.[197]

Ariel Dobkin proposes a more granular framework, arguing that informational fiduciary duties should be divided into four categories of behavior: manipulation, discrimination, sharing with third parties without consent, and violations of a company's privacy policy.[198] A duty is violated when the fiduciary exceeds a reasonable user's expectations, which those types of conduct will generally do.[199] These four types of conduct are more specific elaborations of the broader fiduciary duties—duties of confidentiality and loyalty would likely cover violations of the company's privacy policy, for example. Dobkin's discussion of duties not

192. BALKIN, *supra* note 26, at 13.

193. Jack Balkin, *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. 1218, 1229 (2016).

194. *Id.* at 1229–30.

195. Zittrain, *supra* note 15, at 340.

196. Data Care Act of 2018, S. 3744, 115th Cong. §§ 2–3 (2018) [hereinafter Data Care Act].

197. Richards & Hartzog, *supra* note 19, at 457–58.

198. Dobkin, *supra* note 29, at 17.

199. *Id.*

to discriminate or manipulate also demonstrates how fiduciary duties would protect against not just privacy harms, but a broader definition of digital injuries, as does Balkin's inclusion of manipulation and discrimination from the kinds of harms his framework would prohibit, and Zittrain's description of "digital gerrymandering."[200] These proposals reflect the range of what an information fiduciary framework could incorporate in terms of scope, ambition, and stringency.

D. Expand the Definition of Digital Harm, and Who Can Be Held Responsible for It

The proposals discussed above offer a variety of approaches to direct and negligent harms, and the types of digital harms that information fiduciary duties would prohibit. In order to effectively guard against the full gamut of digital harms not covered by existing law, an information fiduciary framework must expand the notion of digital harm beyond unauthorized disclosure of information, and physical and monetary harms—indeed, beyond privacy. In addition, the architecture of the online ecosystem requires an approach to fiduciary duties that does not focus on direct conduct alone: fiduciaries should also not be permitted to enable the manipulation, discrimination, or privacy violations of users stemming from unreasonably lax enforcement of their own policies, or design choices that enable those harms. The following Sections will address how fiduciary duties could incorporate a more expansive definition of privacy harms, including a broader definition of digital harms more generally, such as discrimination and manipulation, and how fiduciaries could be applied to address the problem of diffuse responsibility.

1. Diffuse Responsibility

For an information fiduciary framework to be effective, it will need to respond to the way large platforms, smaller players, and third-party services create a tangled web of interactions resulting in direct and indirect harms to users. In addition, the negligence of internet platforms in policing the spaces they provide for misconduct has led to a slew of problems, and an effective information fiduciary framework must tackle not only the direct actions of data collectors, but also the harms that passivity can perpetuate. Architectural choices that facilitate user harms and failure to enforce a service's policies often overlap, and the result is platforms that facilitate harassment, manipulation, and discrimination, thanks to a negligent failure to see how products built for good can easily be used for

200. Zittrain, *supra* note 15, at 335.

evil, along with a healthy dose of monetary self-interest.[201] For a few examples, Twitter's lax enforcement and opaque policies concerning harassment have led women, activists, and other targeted groups to leave the site rather than endure the abuse[202]—or continue to endure the slurs and death threats at great effort, cost, and risk to their personal safety.[203] Design choices on Airbnb led to widespread problems of bias on that platform.[204] And Facebook's failure to devote sufficient resources to content moderation in Myanmar contributed to a violent genocide.[205]

Platforms turning a blind eye as third parties violate their policies or otherwise hurt users is a big part of how companies may indirectly perpetuate harms. Certainly, lax enforcement makes perfect sense in an environment where platforms want as many users as possible, as many app purchases as possible, and as many ad clicks as possible.[206] Established companies want to entrench their dominant positions, while up-and-comers want to join their ranks or establish metrics to secure the next round of funding. Problems like a recommendation algorithm that suggests ever more extreme content[207] or accounts that create high levels of engagement through harassing other users pose a collateral risk while contributing to tech companies' bottom lines.[208] Meanwhile, tech companies promise to do better, but fail to make meaningful changes because the status quo is more profitable. A fiduciary framework should consider how companies can make their services and products safely usable by everyone, not just those with the wherewithal to survive the

---

201. *See, e.g.*, Ari Ezra Waldman, *Manipulating Trust on Facebook*, 29 LOY. CONSUMER L. REV. 175, 185 (2017) ("Facebook has a strong financial interest in not only what we share, but in encouraging us to share as much personal information as possible: the more data it has, the better it can target its ads, and the more revenue it can earn."); Mark Bergen, *YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant*, BLOOMBERG (Apr. 2, 2019), https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant (describing "corporate leadership unable or unwilling to act on these internal alarms [regarding how the YouTube algorithm inculcated and spread extremist content] for fear of throttling engagement").

202. Simon Parkin, *Gamergate: A Scandal Erupts in the Video Game Community*, NEW YORKER (Oct. 17, 2014), https://www.newyorker.com/tech/annals-of-technology/gamergate-scandal-erupts-video-game-community [https://perma.cc/7JNK-RULN].

203. Sarah Jeong (@sarahjeong), TWITTER (Dec. 18, 2018, 1:28 PM), https://twitter.com/sarahjeong/status/1075140792765734912 [https://perma.cc/WC8W-7CNQ].

204. *See* Levy & Barocas, *supra* note 166.

205. *See generally* LEWIS, *supra* note 126.

206. *See, e.g.*, Nicholas Confessore & Gabriel J.X. Dance, *On Social Media, Lax Enforcement Lets Imposter Accounts Thrive*, N.Y. TIMES (Feb. 20, 2018), https://www.nytimes.com/2018/02/20/technology/social-media-impostor-accounts.html [https://perma.cc/8VBL-3L3P].

207. *See, e.g.*, Zeynep Tufekci, *YouTube, the Great Radicalizer*, N.Y. TIMES (Mar. 10, 2018), https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html [https://perma.cc/QTW6-S5AX].

208. *See, e.g.*, Confessore & Dance, *supra* note 206.

inevitable toxicity, particularly when the harms may not be fully avoidable by anyone.

As implemented in a fiduciary framework, a prohibition on negligently creating or incentivizing a dangerous environment would likely come under the duties of care or loyalty. The Data Care Act defines the duty of loyalty as prohibiting fiduciaries from using "individual identifying data or data derived from individual identifying data" in a way that would "benefit [the fiduciary] to the detriment of the end user" if it would "result in reasonably foreseeable and material physical or financial harm to an end user" or "be unexpected and highly offensive to a reasonable end user,"[209] one or the other. That definition of harm is fairly narrow, and should not be limited to physical or financial injuries. Dignitary and other harms that are not necessarily physical or financial could also be "unexpected and highly offensive to the reasonable person," but given the difficulty of accurately gauging digital mores—and how high the threshold of "highly offensive" could be set—the bill's definition of harm should be more capacious.

2. Privacy Harms

In addition to expanding the notion of legally cognizable digital harms, an effective information fiduciary framework should expand the definition of what a privacy harm is. It should also strengthen existing protections, such as more meaningful obligations to enact reasonable security protocols, and stricter requirements to notify users in the case of breach. These objectives could be met by a combination of the duties of care, loyalty, and confidentiality. A data breach resulting from unauthorized access to a poorly secured system is one harm that would likely be both squarely prohibited by fiduciary duties and firmly within what U.S. privacy law already prohibits.[210] The duty of care under the Data Care Act, for example, is primarily focused on a federal standard (and different application) of securing data and breach notifications, which are already covered by a range of laws.[211] Richards and Hartzog argue that the duty of confidentiality could be parsed into different levels of obligation in order to better tailor the traditional duty for the data collector context,

209. Data Care Act, *supra* note 196, § 3(b)(2).

210. *See generally Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/XL5D-S863].

211. The Data Care Act's duty of care requires service providers to "reasonably secure individual identifying data from unauthorized access" and "promptly inform" users in the case of unauthorized access to individually identifying information under the duty of care. Data Care Act, *supra* note 196, § 3(b)(1).

which they divide into "nondisclosure, limited disclosure, trustworthy recipients, and obfuscation to be discreet."[212]

Additionally, an effective information fiduciary framework should not make the definition of a privacy harm contingent on physical or monetary injury. While the FTC's efficacy has been limited by a lack of civil penalty authority and a greater need for resources, it is also hamstrung by a limited approach to defining informational harm, despite the fact that many digital harms do not involve financial loss or necessarily involve an imminent risk to physical safety.[213] In other cases, with an FTC more inclined to protect industry over consumers, a narrow definition of informational injury simply provides an excuse for anemic enforcement.[214] Expanding the definition of what constitutes a privacy harm to more broadly include non-financial injuries is particularly crucial as so many digital products and services do not require users to pay for the service.[215] Provided the definition was not unnecessarily cabined to financial or physical harm,[216] a duty of confidentiality would extend to privacy invasions that the FTC has appeared to not consider within its purview because of its narrow interpretation of informational injury.

The GDPR provides a broad definition for cognizable injury, as any data subject has "the right to an effective judicial remedy where he or she considers that his or her rights . . . have been infringed" as the result of processing, or as the result of a company not complying with the law,[217] and violating any of the GDPR's many requirements for providers and specific rights for consumers could constitute grounds for a hefty fine.[218] A fiduciary framework would likely not expand the basis for a cognizable privacy harm quite that far, and would be somewhat limited by courts' application of *Spokeo*.[219]

The duty of care, confidentiality, or loyalty would prohibit many of the invasive practices permitted under current law, or which go unpunished by an under-resourced, or simply inert, FTC. A key change to

212. Richards & Hartzog, *supra* note 19, at 460–61.

213. *See supra* Section II.C.

214. Confessore & Kang, *supra* note 84 (noting that an FTC official rejected the concerns of his staff over undisclosed location tracking by "respond[ing] that the tech companies were legitimate businesses offering free services, and it was unclear how they had harmed consumers").

215. *Id.*

216. *Cf.* Data Care Act, *supra* note 196, § 3(b)(2).

217. GDPR, *supra* note 70, art. 79(1), at 80.

218. *Id.* art. 83(2)–(5), at 82–83; *see also* Hoofnagle et al., *supra* note 102, at 93.

219. *See* Solove & Citron, *supra* note 115, at 743–44 (detailing *Spokeo*'s holding that courts must find an injury in fact for plaintiffs to have standing to sue); *id.* at 761–74 (explaining the legal basis for how risk and anxiety stemming from data breach constitute such an injury); *see also* Matthew S. DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2468 (discussing new theories of privacy harms a post-*Spokeo* court could rely on).

privacy enforcement would be the current challenge of relying on deception to effectively regulate privacy, which can leave no legal recourse for victims simply because a company informed them (in fine print, of course) that it could invade their privacy.[220] As duties of care, loyalty, and confidentiality would protect users regardless of whatever fine print obfuscation companies use to attempt to trick them, a fiduciary framework could actually improve upon the GDPR's attempts to fix notice and choice.[221]

Fundamentally, a higher legal obligation to users would help shift the default attitude of data collectors from "collect everything and ask questions later," as would holding the service provider responsible for enabling privacy invasions by third parties. As both Balkin and the Data Care Act propose, fiduciaries should be required to contractually obligate any third parties they share data with to uphold the fiduciary duties they owe their users.[222] As Balkin puts it, "fiduciary obligations must run with the data."[223] As one small example, Facebook reportedly shared user information with so many third parties that many were unaware that they even had access to so much information.[224] Affirmative legal duties to users, like a prohibition on sharing their information except with entities required to uphold the fiduciary's same duties, would vastly limit incentives to share information as recklessly as companies like Facebook have. Companies that serve as a data hose to other services—Google, Facebook, data brokers, and other entities—would also bear a responsibility to the individuals whose data they are sharing that it would not be used to their detriment. This resembles the GDPR's holding data collectors responsible for the actions of the entities it contracts with,[225] as well as the law's disfavoring of third-party data sharing.[226]A broader definition of privacy harms and a shift in the default assumption that a company owes duties to its users, as opposed to a default that they do not, would be a key shift in the balance of power between individuals and the companies taking advantage of them.

---

220. *See* Brookman, *supra* note 65, at 358–59 (describing the FTC's approach to deception as creating an enforcement regime of "don't go out of your way to lie about what you do" and that even despite relatively increased vigilance from the FTC, it lacks "the capacity by itself to enshrine all of the Fair Information Practice Principles into U.S. law").

221. BALKIN, *supra* note 26, at 14.

222. Data Care Act, *supra* note 196, § 3(b)(3); *see also* BALKIN, *supra* note 26, at 3.

223. BALKIN, *supra* note 26, at 13.

224. Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html?module=inline [https://perma.cc/2EDU-B6PQ].

225. Hoofnagle et al., *supra* note 102, at 68; *see also id.* at 96.

226. *Id.* at 74.

3. Beyond Privacy Harms: Manipulation & Discrimination

In addition to expanding the kinds of legally cognizable privacy harms, an information fiduciary framework should also address manipulation and discrimination in order to ensure that people are protected from the full array of modern digital threats that they face. While defining manipulation can be fraught, certain attributes can be combined to a definition that the law should prohibit without being severely over-inclusive. Building on Ryan Calo's work on digital manipulation, Ido Kilovaty argues that the kind of manipulation that should be subject to legal limitations is hidden from the subject, exploits the subject's vulnerabilities, is targeted to her with the objective of changing her behavior or outlook, and warrants intervention when the manipulator is leveraging her divergent interests over the subject.[227] Dobkin highlights two definitions of problematic manipulation: conduct that ignores the dignity or autonomy of the subject and conduct that subverts the welfare of the user to the welfare of the data collector when their interests diverge.[228] Balkin provides yet another definition, characterizing 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."[229] As Balkin and others argue, while manipulation is hardly new as a commercial concept, digital companies have the ability and incentive to manipulate their users in a particularly dangerous and impactful way.[230]

These definitions all contribute important facets to what a definition of manipulation should include. I would argue that persuasive tactics targeted to the user, designed to exploit her vulnerability and intended to change her conduct or outlook when the interests of the subject and the provider diverge, should constitute manipulation and violate the duty of loyalty. Manipulation that preys on normative values like autonomy, equality, and dignity could exacerbate the egregiousness of the violation, as would manipulation based on a protected group status or activity. Manipulation for ideological purposes, commercial purposes, or both would violate the duty. Given the diffuse nature of networked products and services, hosting a platform or service that facilitates manipulation by

227. Ido Kilovaty, *Legally Cognizable Manipulation*, BERKELEY TECH. L.J. (forthcoming 2019) (manuscript at 16) (on file with Berkeley Technology Law Journal) (discussing different definitions of manipulation and the worthiness of each of legal intervention); *see also id*. at 18 (citing Calo, *supra* note 79, at 1023). Kilovaty further argues that his proposal to recognize certain kinds of manipulation as a harm under data breach laws would accomplish goals similar to Balkin's fiduciary framework. *Id*. at 45–46.

228. Dobkin, *supra* note 29, at 19.

229. BALKIN, *supra* note 26, at 4.

230. *Id.* at 4–5.

other users or by third parties could sometimes violate the duty of loyalty, and should generally violate the duty of care.

As an example, an entity that purports to provide a "neutral" product or service but quietly subjects users to a deliberate ideological campaign would be engaging in manipulation that should violate the duty of loyalty. Pushing an ideological agenda with the objective of changing the user's perception of an issue or shaping their actions is the company placing its welfare above that of its users, based on the user's lack of awareness of the service's ultimate objective. As an example, Dobkin describes the hypothetical of Walmart promoting an anti-abortion agenda by configuring its website to direct ads featuring "adorable babies" if the user searches for "birth control," and says that scenario would not violate her principle of anti-manipulation if the company was subjecting all users to those tactics rather than some.[231] That framing conflates manipulation with discrimination, and the latter should not have to exist for the former to be found. Moreover, targeting can be implicit: Walmart can easily bank on the assumption that women of child-bearing age seeking information about contraception are a sizeable proportion, if not the majority, of the users searching its site for "birth control." Deliberate, obfuscated ideological skewing of a purported neutral service should be considered manipulation of the user and a violation of the duty of loyalty.[232] Companies should not be able to surreptitiously subject their users to campaigns of ideological manipulation, and individuals should be able to hold them legally responsible if they do.

Distinguishing manipulation that exploits vulnerabilities and is based on subverting the user's interests to the company's divergent ones still allows companies to conduct legitimate forms of persuasion—generally speaking, non-exploitative advertising, or product architecture that does not seek to exploit users' vulnerabilities for the company's benefit. An advertiser, or the operator of the site hosting the ad, should not be able to target a user with ads for casinos based on her searches for the nearest Gamblers Anonymous meeting. This surreptitiously exploits a vulnerability of the user to the advertiser's benefit and the user's detriment. But a company could, for example, target a user on a contextual basis by sending her an ad for Gatorade, a sports drink, because she is reading an article on how to avoid dehydration in sports, or streaming a sporting event. This attempt to persuade the user for the company's gain—either the publisher or the advertiser—did not exploit the user's

231. Dobkin, *supra* note 29, at 21–22.

232. *See also* Zittrain, *supra* note 15, at 340 ("However agreed, a central responsibility of an information intermediary would be to serve up others' data in ways not designed to further the political goals of the intermediary.").

vulnerability or surreptitiously perform one function while insidiously accomplishing another to the company's benefit and her detriment.[233]

As discussed above, a data collector can attempt to manipulate users directly, or it can enable or facilitate manipulation by third parties, and an effective fiduciary framework would address both. Information fiduciaries enabling manipulation by third parties, such as through search results that prioritize misinformation, could violate the duty of loyalty or care. For example, reporting by April Glaser echoed a version of Dobkin's hypothetical when she demonstrated that YouTube consistently surfaces search results for "abortion" that reflect anti-abortion disinformation.[234] Unlike Dobkin's hypothetical, the ideological skew of the abortion results on YouTube is due to the content uploaded by users of that platform, the architecture of how its algorithm rewards engaging content,[235] and lack of enforcement,[236] rather than the result of an ideological agenda being pushed by YouTube itself. But as noted above, this kind of negligence can still have dangerous effects if users take the disinformation at face value,[237] and in certain cases, it may be appropriate to hold platforms responsible for patterns of reckless disregard for how third parties are manipulating the platform. Disinformation about vaccinations fits a similar profile of potential harm created by a platform that fails to crack down on misinformation and users who do not realize the information they are being provided is false.[238]

Another example of an ideologically manipulative practice would be attempting to surreptitiously influence users regarding whom they should

---

233. *See* BALKIN, *supra* note 26, at 12–13.

234. April Glaser, *YouTube's Search Results for "Abortion" Show Exactly What Anti-Abortion Activists Want Women to See*, SLATE (Dec. 21, 2018, 3:32 PM), https://slate.com/technology/2018/12/youtube-search-abortion-results-pro-life.html [https://perma.cc/D52U-WERF].

235. Tufekci, *supra* note 207; *see also* Jack Nicas, *How YouTube Drives People to the Internet's Darkest Corners*, WALL ST. J. (Feb. 7, 2018, 1:04 PM), https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478 [https://perma.cc/E3WJ-2FL7].

236. Andy Kroll, *John Podesta Is Ready to Talk About Pizzagate*, ROLLING STONE (Dec. 9, 2018), https://www.rollingstone.com/politics/politics-features/john-podesta-pizzagate-766489/ [https://perma.cc/F4EB-VM8N]; *see also* Glaser, *supra* note 234.

237. *See* Ben Collins, *Posing as Gay Men on Twitter, a Troll Goes Viral with Attempts to Falsely Tie the LGBTQ Community to Pedophilia*, NBC NEWS (Jan. 4, 2019), https://www.nbcnews.com/tech/tech-news/posing-gay-men-twitter-troll-goes-viral-attempts-falsely-tie-n954721?cid=sm_npd_nn_tw_ma [https://perma.cc/RE9M-8PJS] (describing how trolls on Twitter stole the identities of gay travel bloggers in an attempt to create and spread false evidence of a connection between homosexuality and pedophilia; only to have their disinformation picked up and reported by far-right news sites and public figures).

238. Jessica Glenza, *Russian Trolls 'Spreading Discord' Over Vaccine Safety Online*, GUARDIAN (Aug. 23, 2018), https://www.theguardian.com/society/2018/aug/23/russian-trolls-spread-vaccine-misinformation-on-twitter [https://perma.cc/WDM5-83B2] ("The vast majority of Americans believe vaccines are safe and effective, but looking at Twitter gives the impression that there is a lot of debate.").

vote for,[239] or allowing third parties to do that.[240] The first would be a violation of the duty of loyalty whereas the second could violate loyalty or care, depending on whether the third-party manipulation resulted from a partnership with the fiduciary or was simply facilitated by its negligent design and oversight.

Other types of manipulation attempt to surreptitiously sway users' actions to the benefit of the collector and the detriment of the subject for solely commercial gain. Some products or services employ "dark patterns"—the architecture of a digital product or platform designed to induce certain behavior—in order to coax more information from the user than she would otherwise share,[241] to persuade the user to use the service for longer or engage with more users while using the service, to spend more money, or to only spend money on certain products.[242] In a particularly bleak example, Facebook reportedly told advertisers it could identify teens who felt "worthless" and "useless," presumably so that they could be targeted for advertisements based on that vulnerability.[243] Balkin argues that attempts by tech companies to make their products and services "addictive" should also violate the duty of loyalty as a form of manipulation.[244]

Discrimination—whether directly perpetrated by the product or service or merely facilitated by it—could also violate the duty of care, loyalty, or both. Unlike with manipulation, a definition that requires the fiduciary to benefit from the detriment in order for a violation to exist would likely be unacceptably narrow. In context, an anti-discrimination principle is not foreign to fiduciary codes; the ethical rules for both

---

239. Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/Y3JJ-WY3T]; *see also* Dobkin, *supra* note 29, at 25.

240. DiResta et al., *supra* note 123.

241. *See generally* FORBUKERRADET, DECEIVED BY DESIGN (2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [https://perma.cc/WK94-WG99]; Waldman, *supra* note 201, at 177 ("But Facebook also uses design tactics that leverage the trust we have in our friends to manipulate us into sharing personal information with websites, advertisers, and third party partners we've never met or heard of. When it does, Facebook crosses the line from carmaker into carjacker, from a conduit of social sharing to a manipulative for-profit scheme where users are reduced to the terabytes of data they generate.").

242. FORBUKERRADET, *supra* note 241, at 6; *see also* Laura Stevens, Sharon Terlep & Annie Gasparro, *Amazon Targets Unprofitable Items, with a Sharper Focus on the Bottom Line*, WALL ST. J. (Dec. 16, 2018, 7:55 PM), https://www.wsj.com/articles/amazon-targets-unprofitable-items-with-a-sharper-focus-on-the-bottom-line-11544965201 [https://perma.cc/YSQ5-LSZV].

243. Sam Levin, *Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure' and 'Worthless'*, GUARDIAN (May 1, 2017), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens [https://perma.cc/ZG5S-P49K].

244. BALKIN, *supra* note 26, at 14.

lawyers[245] and doctors[246] incorporate responsibilities to avoid discrimination in order to ensure equitable access to their services. Dobkin proposes that fiduciaries would be required to adhere to an anti-discrimination principle, and taxonomizes three primary modes of digital discrimination: access to services, different prices, and refusing to offer a service in a certain area, with geography serving as a proxy for race ("digital redlining").[247]

In some cases, it may be relatively easy to demonstrate that a fiduciary is engaging in discrimination, as it continues to profit from a service that the company is aware is having discriminatory effects.[248] The kind of "engaging" content that tech companies are incentivized to promote can often include racist or sexist content or harassment based on protected attributes, such as gender or race.[249] Thus, a company's failure to put the safety of its users over revenue or lax enforcement has disproportionate effects for the targets of harassment or the users whom an under-enforced policy was designed to protect.[250] And just as a prohibition on manipulation as described above would not prohibit all targeted advertising, the application of the duty of loyalty or care to exclude discrimination would not prevent every way in which a service provider treats one group differently from another based on immutable characteristics, or adherence to a certain group. For example, a dating app would not be enabling discrimination by permitting users to only receive "matches" or messages from members of the genders they prefer, as opposed to mandating that all users receive matches from all genders. But a dating app that allowed users to search for matches based on ethnicity would likely be enabling discrimination.[251] As demonstrated by the

245. *See, e.g.*, Myles V. Lynk, Professor of Law, Ariz. State Univ., Presentation to the Labor & Employment Law College: Discrimination & Harassment in the Profession: A New Ethics Rule (Nov. 10, 2018), https://www.americanbar.org/content/dam/aba/events/labor_law/2018/AnnualConference/papers /Ethics%20Rule%20on%20Discrimination.pdf [https://perma.cc/7A9S-ZC2X].

246. *See, e.g.*, Danielle Hahn Chaet, *AMA Code of Medical Ethics' Opinions Related to Discrimination and Disparities in Health Care*, 18 AMA J. ETHICS 1095 (2016).

247. Dobkin, *supra* note 29, at 27.

248. *See, e.g.*, Nancy Leong & Aaron Belzer, *The New Public Accommodations: Race Discrimination in the Platform Economy*, 105 GEO L.J. 1271 (2017) (arguing that public accommodations laws should extend to discrimination from users, and to the extent that they do not, suggest modifications).

249. SYLVAIN, *supra* note 126, at 3–4 ("Intermediaries, moreover, design their platforms in ways that shape the form and substance of their users' content . . . [and] should not get a free pass for enabling unlawful discriminatory conduct.").

250. *Id*. at 9 ("[T]he victims of online abuse tend to be the same sorts of people who have always been subject to attack and harassment offline in the United States and elsewhere—in particular, young women, racial minorities, and sexual 'deviants.'").

251. *See generally* Jevan Hutson et al., *Debiasing Desire: Addressing Bias & Discrimination on Intimate Platforms*, 2 PROC. ACM HUM.-COMPUTER INTERACTION 73 (2018) (describing dating platforms that have been criticized for facilitating discrimination).

volume of bad faith arguments raised in recent years about a non-existent specter of bias against conservative political views on online platforms,[252] any definition of discrimination should take care in establishing a standard of proof and defining the relevant standard of care.

It is likely that manipulation and discrimination will often be found together, though again, the one should not require the other. While targeting certain users might exacerbate the degree of the violation of the duty of loyalty, it should not be necessary for manipulation to take place. For example, Facebook's subjecting black users to be disproportionately targeted by Russian disinformation agents in order to persuade them not to vote for Hillary Clinton,[253] on top of the company's ignoring the needs of black users[254] and being insufficiently cooperative with Senate investigations into interference with their platforms,[255] would likely violate the duties of care and loyalty. Given that the people being targeted were selected on the basis of race, this could constitute both discrimination and manipulation, particularly given that the purpose of the manipulation was to deter people from voting, a protected activity. In contrast, Facebook making it appear as though users had notifications they couldn't access until they accepted its new terms and conditions is no less manipulative for targeting all users instead of a subset of them[256] because it surreptitiously exploited its users to their detriment, and to its benefit.

---

252. Brian Feldman, *Twitter Is Not 'Shadow Banning' Republicans*, N.Y. MAG. (July 25, 2018), http://nymag.com/intelligencer/amp/2018/07/twitter-is-not-shadow-banning-republicans.html [https://perma.cc/688X-3TH3]; Colby Itkowitz, *Congersswoman to Google CEO: Why When I Search 'Idiot' Do I Get Pictures of Trump?*, WASH. POST (Dec. 11, 2018), https://www.washingtonpost.com/politics/2018/12/11/congresswoman-google-ceo-why-when-i-search-idiot-do-i-get-pictures-trump/?utm_term=.cb7b5a9424da [https://perma.cc/AYD7-22RG] (describing how in subsequent House hearing, "Republicans on the panel couldn't get past the myth that some person(s) inside Google couldn't arbitrarily change search algorithms for political gain."); Alyssa Newcomb & Ben Collins, *House Republicans Float Online Conspiracy Theories in Hearing About Social Media 'Censorship'*, NBC NEWS (July 17, 2018), https://www.nbcnews.com/tech/tech-news/house-republicans-float-online-conspiracy-theories-hearing-about-social-media-n892206 [https://perma.cc/2UNJ-ADHW] (detailing the House Judiciary Committee Hearing on purported bias on tech platforms, and the lack of evidence to support the claims by congressional Republicans of bias or ideological censorship); Laura Hazard Owen, *Twitter's Not "Shadow Banning" Republicans, but Get Ready to Hear That It Is*, NIEMANLAB (July 27, 2018), http://www.niemanlab.org/2018/07/twitters-not-shadow-banning-republicans-but-get-ready-to-hear-that-it-is/ [https://perma.cc/JZZ7-TU2P]; Nicholas Thompson & Fred Vogelstein, *Inside the Two Years That Shook Facebook—And the World*, WIRED (Feb. 12, 2018), https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/ [https://perma.cc/NEU5-4W7C] (describing allegations of bias against conservatives at Facebook and the lack of basis for them).

253. DiResta et al., *supra* note 123, at 8.

254. *See* Mark S. Luckie, *Facebook is Failing Its Black Employees and Its Black Users*, FACEBOOK (Nov. 27, 2018), https://www.facebook.com/notes/mark-s-luckie/facebook-is-failing-its-black-employees-and-its-black-users/1931075116975013/ [https://perma.cc/8WYG-PZ5J]; Riley, *supra* note 175.

255. DiResta et al., *supra* note 123, at 5, 33.

256. FORBUKERRADET, *supra* note 241, at 28.

Some conduct might violate multiple duties at once. For example, various combinations of lax enforcement, direct manipulation, or enabled manipulation might violate both the duty of loyalty and the duty of care. Consider Google's Play Store, which forbids developers who participate in its "Designed for Families" program to use "overly commercially aggressive tactics" on child users.[257] Yet in a white paper by Google-owned AdMob, the digital advertising company advises developers on how to wring the most revenue out of its users, including "motivating" users who are "stuck" on a level.[258] In a letter and subsequent complaint to the FTC, child advocates discussed how developers have used those very techniques in apps targeted to children in order to maximize revenue, such as making a puppy cry unless the user purchases accessories for her or having a well-loved children's character express her disappointment that the child did not purchase an in-app skill.[259] This kind of tactic manipulates children, whose judgment and understanding of commercial tactics are less developed than those of adults.[260] One developer quoted in the AdMob whitepaper, TabTale, was found to employ those types of techniques in its child-directed apps.[261] Google's failures to enforce its Play Store policies would violate the duty of care, while its proactive encouragement, via its subsidiary AdMob, that developers try to manipulate its users into spending more money in Play Store apps would seem to violate the duty of loyalty. That Google was encouraging a developer that primarily makes children's apps, and offers its children's apps on the Play Store, to implement this manipulative technique also seems discriminatory towards children.

257. Complaint at 37–38, Request to Investigate Google's Unfair and Deceptive Practices in Marketing Apps for Children, Submitted to the F.T.C. by the Institute for Public Representation at Georgetown Law on behalf of Campaign for a Commercial-Free Childhood, Center for Digital Democracy, and Others (Dec. 19, 2018) (describing "overly aggressive commercial tactics"); *see also id*. at 14–16 (describing how AdMob incentivizes and facilitates such tactics).

258. Sean Meng, *Charge Your Game Monetization with a Winning Combination of In-App Purchases and Ads*, GOOGLE ADMOB (Dec. 1, 2015), https://www.blog.google/products/admob/charge-your-game-monetization-with-admob/ [https://perma.cc/LE82-SZQH].

259. *See* Complaint, *supra* note 257, at 37–42; Press Release, Campaign for a Commercial-Free Childhood, Advocates Ask FTC to Investigate Apps Which Manipulate Kids (Oct. 29, 2018), www.commercialfreechildhood.org/advocates-ask-ftc-investigate-apps-which-manipulate-kids [https://perma.cc/PL7C-CGJR].

260. Marisa Meyer et al., *Advertising in Young Children's Apps: A Content Study*, 40 J. DEV. BEHAV. PEDIATR. 32, 32 (2018) (citing J. Howard Beales, *Advertising to Kids and the FTC: A Regulatory Retrospective That Advises the Present*, FED. TRADE COMM'N (2004), https://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kids-and-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf [https://perma.cc/K2TU-Y6M7].

261. Complaint, *supra* note 257, at 37–42.

V. FURTHER CONSIDERATIONS

While the idea of applying fiduciary duties to data collectors has grown in popularity,[262] it has also been subject to critique, notably by Khan and Pozen in their essay *A Skeptical View of Information Fiduciaries*.[263] While I share their skepticism towards the efficacy of an opt-in fiduciary regime, I do respectfully disagree with them on other points. Broadly, the authors argue that a fiduciary approach precludes badly needed structural reforms, and that it would reify the dominance of platform companies rather than eroding it, while strengthening an illusion of those companies' trustworthiness that should instead be shattered.[264] I believe a mandatory framework that creates significant obligations and prohibitions for data collectors would deter the kind of digital exploitation that the current ecosystem incentivizes, particularly when bolstered by an impactful enforcement regime and avenues for individuals to both exercise their rights and sue on the basis of their violation. It likely would not accomplish sweeping competition-focused reforms, but it does not purport to. Nor does it preclude additional statutory or regulatory competition-focused reforms, which I agree are needed.[265]

The critique that a trust-focused approach might inure the perception of data collectors from the skepticism they deserve[266] is also well-taken, though it again assumes the more conciliatory model of an opt-in regime that I agree is insufficient. The entire basis of fiduciary law is the assumption that fiduciaries are incentivized to take advantage of their clients unless the law somehow changes that calculus, such as by prohibiting self-dealing.[267] The language of trust is not an empty assurance, or a congratulatory description that assumes that information fiduciaries have earned the trust they have been given: rather, it invokes the gravity of the obligation that U.S. privacy law has not previously required them to meet. The compulsory nature of the fiduciary status and robust enforcement of violations assumes inevitable abuse of that trust,

---

262. Khan & Pozen, *supra* note 179, at 3–4.

263. *Id*. at 29–30.

264. Or as Khan and Pozen eloquently put it, "a framework, we fear, invites an enervating complacency toward online platforms' structural power and a premature abandonment of more robust visions of public regulation." *Id.* at 1.

265. Balkin argues for how such reforms would be complementary to the objectives of a fiduciary framework. BALKIN, *supra* note 26, at 10–11; *id.* at 15 ("The fiduciary approach also meshes well with other forms of consumer protection, and it does not exclude other reforms, like GDPR-style privacy regulation. In particular, it does not get in the way of new pro-competition rules or increased antitrust enforcement as described above.").

266. Khan & Pozen, *supra* note 179, at 27.

267. Frankel, *supra* note 12, at 825 (describing the motivation behind court-fashioned fiduciary duties as an "acknowledge[ment of] the frailty of human nature").

rather than presuming that data collectors deserve it and should not be scrutinized.[268]

Khan and Pozen also argue that a business model based on behavioral advertising is fundamentally incompatible with a duty to put the well-being of users first, which takes a narrow view of the types of business models that a fiduciary framework would hope to modify. While many of the abuses that a new law would hopefully fix stem from business models that are inherently harmful, others are the unintended consequence of the skewed priorities in an ecosystem with few applicable laws and limited enforcement. The issue is not always an intrinsically venal business model, but also ones where it is too easy for companies to leave questions of whether their product enables discrimination, manipulates users, or is likely to instigate third party misuse at the end of the product design cycle, rather than at the beginning.[269] That critique also overlooks the transformative effect that shifting to the presumption that data collectors are responsible to their users, from the presumption that they generally are not, would have for the holes, lapses, and inefficacies of existing privacy law. And as noted *supra*,[270] traditional fiduciary relationships also suffer from similarly recurring conflicts—the acknowledgement of inherent conflicts, and a desire to deter fiduciaries from taking advantage of them, is the fundamental premise of a fiduciary framework.

The objective of this Article is not to suggest that fiduciary duties are necessarily a better approach than a system based on a constitutional right to privacy and data protection against private entities in a magical land where the U.S. Constitution contained such a specific right, or if scholars were to devise a sufficiently convincing theory that it does.[271] Nor is it to suggest that an information fiduciary approach and the regulatory vision of the GDPR are mutually incompatible.[272] They share many objectives, like protecting the dignity, autonomy, and privacy of individuals in the digital age, and certain approaches, such as significantly disincentivizing

---

268. Frankel, *supra* note 12, at 804 ("[A]ll [fiduciary relationships] require the fiduciary to use delegated power to facilitate his service to the other. All pose the possibility of abuse of that power.").

269. This of course echoes the objectives of GDPR's Article 25 requirement of privacy by design. ("[T]he controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures . . . which are designed to implement data-protection principles . . . in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."). GDPR, *supra* note 70, art. 25(1), at 48.

270. *See supra* Section IV.A.

271. They haven't yet. *See* McGeveran, *supra* note 7, at 976; Schwartz & Peifer, *supra* note 3, at 133–34.

272. As Balkin notes, an information fiduciary framework is not mutually incompatible with the GDPR, nor with pro-competition consumer protection intervention. BALKIN, *supra* note 26, at 15.

misconduct[273] through enhanced enforcement mechanisms. Both approaches attempt to protect individuals against broader classes of harms beyond privacy, such as algorithmic bias.[274] Many U.S. companies do business in Europe and are required to comply with the GDPR; many EU citizens and U.S. customers of EU business have rights under the GDPR.[275] Moreover, the focus of a fiduciary framework on the data collectors—what standards they should be required to meet, and what they should be prohibited from doing—could, and should, include certain affirmative individual rights like the ones the GDPR creates. The duty of loyalty or care, for example, could be written to incorporate any number of the GDPR's individual rights, such as access, correction, and data portability.[276] Many of the GDPR's objectives and legal innovations are laudable, and should be emulated, as U.S. state lawmakers have already begun to do.[277]

But in the U.S. legal system—lacking a constitutional right to privacy against all entities, limited by the First Amendment, and with a strong, historical and philosophical bent towards deregulation—a brick-by-brick recreation of the GDPR is likely unrealistic. An information fiduciary framework can overcome those very roadblocks, while achieving the GDPR's primary objective of restoring individual protections against digital harms.[278] And while Congress certainly does not need to locate a right to privacy against private entities in the Constitution to create one by statute, a fiduciary model injects a moral imperative to

---

273. *See generally* Electronic Frontier Foundation, Comment Letter on the National Telecommunications and Information Administration's Approach to Consumer Privacy (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/11.9.18_comments_of_eff_to_ntia_dkt_180821780-8780-01.pdf [https://perma.cc/9QHD-PGG6] (suggesting that the NTIA adopt both specific provisions to the GDPR, such as data portability, and an information fiduciary approach).

274. GDPR, *supra* note 70, art. 22, at 46; *see also Rights Related to Automated Decision Making Including Profiling*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ [https://perma.cc/N46R-ZY65].

275. GDPR, *supra* note 70, art. 3, at 32–33.

276. Hoofnagle et al., *supra* note 102, at 88–91.

277. *See generally* DATAGUIDANCE, COMPARING PRIVACY LAWS: GDPR V. CCPA (2018), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [https://perma.cc/NR5K-XYCX] (discussing the similarities and contrasts of the California Consumer Privacy Act and the GDPR); Katherine E. Armstrong & Qisui Y. Newcom, *New Washington State Privacy Bill Incorporates Some GDPR Concepts*, NAT'L L. REV. (Jan. 31, 2019), https://www.natlawreview.com/article/new-washington-state-privacy-bill-incorporates-some-gdpr-concepts [https://perma.cc/HSH8-TJMS] (describing a new Washington state bill that includes GDPR-inspired rights); Daniel Kim & Alaap B. Shah, *Follow the Leader: California Paves the Way for Other States to Strengthen Privacy Protections*, LEXOLOGY (Mar. 7, 2019), https://www.lexology.com/library/detail.aspx?g=c5adfa5e-2ae9-4903-82f1-0e06f0bc1e49 [https://perma.cc/9N5E-CB4Y] (discussing privacy bills in eight states looking to both the GDPR and CCPA as inspiration).

278. *See supra* Part I.

digital protections that the U.S. conception of privacy as a good frequently lacks.

Moreover, the balance that fiduciary duties can strike between the legitimate commercial objectives of the provider and protecting the rights of the subject also coalesces with a U.S. privacy framework accustomed to allowing companies to move fast and break things, while preventing companies from breaking them quite so rampantly. It can meet a range of competing objectives without sacrificing the primary goal of strengthening protections for individuals against a range of evolving digital harms. Finally, an information fiduciary framework can coalesce with U.S. laws more easily than a wholesale import of the GDPR, as it can accommodate First Amendment rights that a GDPR clone would violate.[279] Indeed, Balkin's focus in proposing the value of a fiduciary framework was free expression, and how fiduciary duties could accommodate the First Amendment prerogatives of data collectors with privacy rights, not just their commercial objectives.[280]

While an information fiduciary framework would inherently alleviate certain aspects of what ails the U.S. privacy ecosystem, other corrective elements are required for the framework to have its intended effect. First, for any new privacy law to significantly change the skewed balance of power between individuals and data collectors, it must modify the existing incentives for data collectors to ignore the law. In an environment of narrowly defined privacy laws, few private rights of action, a slim likelihood of regulatory enforcement, and tempered consequences in the unlikely event enforcement occurs, companies justifiably assume that the risk of violating the law is lower than the risk of failing to maximize growth and profits. Creating new rights for individuals by characterizing data collectors as information fiduciaries will do nothing without making it expensive or legally risky for companies to violate those rights.

As such, assuming a proposal that still relies on the FTC as the primary privacy enforcement agency, the FTC must be given rulemaking authority and civil penalty authority, as well as more resources and manpower. The likelihood that a regulator will investigate lapses and breaches and that investigation will result in a meaningful fine or injunction must significantly rise for companies to put more resources and thought not only into compliance, but into prevention of misuse. A private

279. Most notably with Article 17's right to erasure, or "the right to be forgotten." GDPR, *supra* note 70, art. 17, at 43–44.

280. Balkin, *Free Speech*, *supra* note 10, at 1154. (describing the concepts of algorithmic nuisance and information fiduciaries as a way to "understand when the First Amendment should allow the state to regulate companies that engage in the collection, analysis, and distribution of data.").

right of action would also push tech companies to invest more heavily in the welfare of its users. Hoofnagle et al. describe the GDPR's objective as putting privacy law on par with the types of law that companies "take seriously"—namely, antitrust and foreign corrupt practices.[281] An information fiduciary framework should do the same.

Finally, expanding the type of harms a fiduciary should be held liable for also necessarily touches on questions of Communications Decency Act § 230.[282] Under that statute's broad liability shield, platform operators are not considered the "publisher or speaker of any information provided" by a third party on their platform and do not bear liability for good faith efforts to restrict certain kinds of harmful content, such as obscenity or harassment.[283] Courts have interpreted § 230 quite broadly, and scholars[284] and advocates[285] have argued that cabining the statute in any way will be the beginning of the end of online free expression and a vibrant internet ecosystem. Defining the harms that platforms should perhaps bear legal responsibility for—even after acknowledging that the harms are egregious—is certainly a delicate exercise,[286] and one that has already gone awry once.[287] But the robust evolution of the online platforms has demonstrated, as Danielle Citron and Ben Wittes memorably put it, that "the internet will not break," if certain modifications are made to the law

281. Hoofnagle et al., *supra* note 102, at 67.

282. 47 U.S.C. § 230 (2018).

283. *Id.* § 230(c).

284. Daphne Keller, *Toward Clearer Conversation About Platform Liability*, KNIGHT FIRST AMEND. INST., https://knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability [https://perma.cc/NX48-ZPPA] (discussing the benefits of § 230 for the development of the internet and urging restraint against "shoot-from-the-hip legislative changes"); Alan Z. Rozenshtein, *Silicon Valley's Regulatory Exceptionalism Comes to an End*, LAWFARE (Mar. 23, 2018), https://www.lawfareblog.com/silicon-valleys-regulatory-exceptionalism-comes-end [https://perma.cc/7ZZ4-MC28] (calling § 230 the "Magna Carta of the internet").

285. *Section 230 of the Communicates Decency Act*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/5CH5-6NXL] ("CDA 230 is perhaps the most influential law to protect the kind of innovation that has allowed the Internet to thrive since 1996.").

286. James Grimmelman, *To Err Is to Platform*, KNIGHT FIRST AMEND. INST., https://knightcolumbia.org/content/err-platform [https://perma.cc/U5VR-3LEC] ("How crisply is it possible to define these categories [of 'good' and 'bad' content on platforms for the purpose of § 230 liability]? . . . Even a 'passive' intermediary has still 'acted' by providing a platform that is a but-for cause of the harm.").

287. Section 230 was recently amended by the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), a move that has been widely criticized by scholars and advocates for the perverse incentives it creates for platforms, and the extent to which it endangers sex workers while purporting to prevent sex trafficking. Danielle Citron & Quinta Jurecic, *FOSTA: The New Anti-Sex-Trafficking Legislation May Not End the Internet, but It's Not Good Law Either*, LAWFARE (Mar. 28, 2018, 2:41 PM), https://www.lawfareblog.com/fosta-new-anti-sex-trafficking-legislation-may-not-end-internet-its-not-good-law-either [https://perma.cc/4ZKF-X9CZ]; Aja Romano, *A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It*, VOX (July 2, 2018, 1:08 PM), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom [https://perma.cc/P6FE-735F].

in light of the harm they have simultaneously enabled.[288] They argue for hinging § 230's liability shield for platforms on their exercise of reasonable care,[289] which would "reduce opportunities for abuses without interfering with the further development of a vibrant internet or unintentionally turning innocent platforms into involuntary insurers for those injured through their sites."[290] One can imagine a similar reworking of § 230 to include an exception to the liability shield when service providers violate the fiduciary duties of care, loyalty, or confidentiality.[291] Olivier Sylvain, for example, argues that courts should account for how design choices enable or cause harm to "predictable targets of harassment and discrimination" when considering whether to extend § 230's liability shield to platform intermediaries.[292] While a full treatment of the issue is beyond the scope of this Article, there is clearly room for certain limitations to § 230's extraordinarily broad liability shield without "breaking the internet."[293]

CONCLUSION

The various interpretations of how fiduciary duties could be applied to data collectors discussed in this Article are united by a common theme: they restore a rights-type valence to a set of relationships that have been reduced to a commercial lens in U.S. privacy policy. Changing the default assumption that individuals are owed nothing by data collectors does not create a constitutional right like the ones undergirding the GDPR, but it does remove some of the obstacles standing between ostensible protections for digital autonomy and a meaningful ability for individuals and regulators to vindicate violations. Without contradicting the value and

288. Danielle Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 401 (2017).

289. *Id.* at 419.

290. *Id.* at 423; *see also* Danielle Citron, *Section 230's Challenge to Civil Rights and Civil Liberties*, KNIGHT FIRST AMEND. INST., https://knightcolumbia.org/content/section-230s-challenge-civil-rights-and-civil-liberties#/_ftnref39 [https://perma.cc/LC7Y-GVBZ]; Ari Ezra Waldman, *Safe Social Spaces*, WASH. U. L. REV. (forthcoming) (manuscript at 49) (on file with Washington University Law Review) (praising the Citron/Wittes proposal and arguing that it would "buttress content moderation designed for user safety and trust").

291. While a full analysis of the intersection is beyond the scope of this Article, it is notable that even Senator Ron Wyden, one of the authors of § 230 and one of its strongest proponents, has suggested that given the strength of the internet ecosystem that developed since the passage of the law and the problems of harassment that companies have failed to account for, it may be time to revisit how limited the platforms' responsibilities are to their users. *See* Colin Lecher, *Sen. Ron Wyden on Breaking up Facebook, Net Neutrality, and the Law That Built the Internet*, THE VERGE (Jul. 24, 2018), https://www.theverge.com/2018/7/24/17606974/oregon-senator-ron-wyden-interview-internet-section-230-net-neutrality [https://perma.cc/9AQW-P49T].

292. SYLVAIN, *supra* note 126, at 3.

293. *See* Danielle Citron, *Sexual Privacy*, YALE L.J. (forthcoming) (manuscript at 66) (on file with Yale Law Journal) ("The call for a more regulated internet is no longer considered outlandish.").

potential of legal arguments for a constitutional right to privacy against private entities under U.S. law, nor arguing that one is needed in order to protect privacy rights by statute, an information fiduciary framework does not require such a right to protect individuals from privacy violations, manipulation, discrimination, and other violations of trust. As fiduciary scholar Tamar Frankel memorably put it, fiduciary duties restore "morality" to legal relationships that lack it.[294]

In some ways, this proposal may sound radical—but so too is the extent to which the scales are tipped. U.S. privacy law needs a radical course correction, not a mere adjustment. A formal classification of data collectors as information fiduciaries simply recognizes the power imbalance that policymakers, academics, and industry can all see exists, and ascribes corresponding obligations to the individuals that the law otherwise permits those entities to exploit.

294. Frankel, *supra* note 12, at 831. ("[T]he emphasis of fiduciary law on morality resulted in elevating the purpose for which the fiduciary's power is granted to a position of priority over other values which may guide the fiduciary. For example, the corporate director's primary duty is to profit for the shareholders; the duty of the attorney is to represent his client's interests; and the duty of the physician is to heal and prolong life. These duties assume a greater moral stature than other, conflicting moral values.").