University of Colorado Law Review

Volume 95 | Issue 1 Article 4

Winter 2024

Data Controllers as Data Fiduciaries: Theory, Definitions & Burdens of Proof

Noelle Wilson

Amanda Reid

DATA CONTROLLERS AS DATA FIDUCIARIES: THEORY, DEFINITIONS & BURDENS OF PROOF

NOELLE WILSON* & AMANDA REID†

As more U.S. states have begun to pass consumer privacy laws, there are growing calls for federal data privacy regulation to ease the burden of compliance with various, sometimes conflicting, state laws. However, scholars and lawmakers are divided on how best to balance robust privacy protections with privacy laws to which businesses can realistically comply. Two prominent regulatory models have emerged from scholarly debate. The Rights/Obligations Model grants consumers various rights and imposes obligations on businesses. This model has been trending in U.S. states, which have mirrored language from the European Union's General Data Protection Regulation (GDPR) by imposing different obligations on "data controllers" and "data processors." However, there are shortcomings to this model that limit consumer rights and their ability to vindicate those rights. The Fiduciary Model has also received attention from lawmakers and scholars as an alternative model of regulation. The Fiduciary Model addresses gaps in the Rights /Obligations Model, but prominent critics have voiced skepticism about the workability of the Fiduciary Model.

This paper's contributions are threefold. First, this paper examines the distinction between "data controllers" and "data processors" in the GDPR and whether those terms are likely to apply in a functionally similar way in new U.S. state consumer privacy laws. As companies strategize about how to

* Noelle Wilson is a Media Law Dual Degree Candidate at University of North Carolina at Chapel Hill, expected to graduate in May 2024 with a J.D. and an M.A. in Media and Communication. Noelle is a graduate research affiliate with the UNC Center for Media Law and Policy and the UNC Center for Information, Technology, and Public Life.

† Amanda Reid is an Associate Professor at the University of North Carolina Hussman School of Journalism and Media, Faculty Co-Director of the UNC Center for Media Law and Policy, and Faculty Research Affiliate at the UNC Center for Information, Technology, and Public Life (CITAP).

comply with laws from a multitude of jurisdictions—and as states incorporate identical language into their own laws—understanding the similarities and differences between how such laws are applied will be crucial. Second, this paper furthers the debate about the workability of the Fiduciary Model by proposing that "data controllers," as defined in the GDPR and U.S. state laws, should be considered "data fiduciaries." This definition offers two benefits: (1) defining data fiduciaries as data controllers provides a workable definition that corresponds with fiduciary theory, and (2) harmonizing U.S. and GDPR law. Finally, this paper will argue that companies subject to state consumer privacy laws should be considered "data controllers" by default and bear the burden of rebutting this presumption. This presumption reinforces the substantive policy behind consumer privacy law, accounts for the probability that parties violating consumer privacy laws will most likely be data controllers, and allocates the burden to the party with superior access to the evidence.

INTRODUCTION

Informational capitalism[1] has been on the rise for decades, exacerbated by the proliferation of new technology and new ways to commoditize attention.[2] Enabled by the aggregation of personal information by tech companies, informational capitalism has given rise to a myriad of societal harms.[3] As more consumer goods are connected to the Internet—like light bulbs, smart TVs, and wearable fitness trackers—security risks increase as well, making it more likely a hacker could access troves of sensitive personal information.[4] Security concerns are exacerbated by concerns about smart devices that listen to users in their homes, even when users are not aware that they are being recorded.[5] Manipulative design practices, referred to as

1. Professor Julie Cohen uses the term "informational capitalism" to refer to the "alignment of capitalism as a mode of production with informationalism as a mode of development." JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 5 (2019) [hereinafter COHEN, BETWEEN TRUTH AND POWER].

2. *See, e.g.*, *id.*; Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460 (2020) (reviewing COHEN, BETWEEN TRUTH AND POWER and SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019)); Shoshanna Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75 (2015).

3. *See, e.g.*, Kapczynski, *supra* note 2, at 1462–63; Shoshanna Zuboff, *You Are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html [https://perma.cc/PT3C-NNNV].

4. *Careful Connections: Keeping the Internet of Things Secure*, FED. TRADE COMM'N (Sept. 2020), https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure [https://perma.cc/C5Q2-VD3S].

5. *See, e.g.*, Yucheng Yang, Jack West, George K. Thiruvathukal, Neil Klingensmith & Kassem Fawaz, *Are You Really Muted? A Privacy Analysis of Mute Buttons in Video Conferencing Apps*, 2022 PROC. PRIV. ENHANCING TECHS. 373

"dark patterns," target consumers and use aggregated data to influence them into making harmful choices like signing up for dubious identity theft protection services, making it difficult to cancel recurring subscriptions and charges, and even performing experiments on consumers.[6] For example, Facebook has experimented on users to influence their emotional states[7] and has been accused of using its algorithms to manipulate its teenage users.[8] In addition, the Cambridge Analytica scandal revealed the potential to harness user data to influence elections.[9]

In light of the many problems stemming from informational capitalism, consumer privacy is becoming a global priority. While the European Union's General Data Protection Regulation (GDPR)[10] is one of the most well-known international privacy laws, many other countries have followed the European Union's lead by passing their own privacy laws.[11]

(2022); Jide Edu, Jose Such, Xavier Ferrer-Aran & Guillermo Suarez-Tangil, *Measuring Alexa Skill Privacy Patterns Across Three Years*, *in* PROCEEDINGS OF THE ACM WEB CONFERENCE 2022 (WWW '22) (April 25, 2022).

6. BUREAU OF CONSUMER PROT., FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT 1, 2 (2022); *see also* Lesley Fair, *Record-Setting FTC Settlements with Fortnite Owner Epic Games Are the Latest "Battle Royale" Against Violation of Kids' Privacy and Use of Digital Dark Patterns*, FED. TRADE COMM'N: BUS. BLOG (Dec. 19, 2022), https://www.ftc.gov/business-guidance/blog/2022/12/record-setting-ftc-settlements-fortnite-owner-epic-games-are-latest-battle-royale-against-violations [https://perma.cc/Z9U9-49M6]; Eur. Data Prot. Bd., *Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them* (Mar. 2022).

7. *See, e.g.*, Kashmir Hill, *Facebook Manipulated 689,003 Users' Emotions for Science*, FORBES (June 28, 2014), https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/?sh=2c6ef227197c [https://perma.cc/DGF7-XERS].

8. *See* Bobby Allyn, *Here Are 4 Key Points from the Facebook Whistleblower's Testimony on Capitol Hill*, NPR (Oct. 5, 2021), https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress [https://perma.cc/JY6D-E2N4].

9. *See, e.g.*, Dipayan Ghosh & Ben Scott, *Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You*, TIME (Mar. 19, 2018), https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data [https://perma.cc/GK77-V3Z9].

10. Regulation 2016/679, of the European Parliament and of the Council of 27 April 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), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

11. *See, e.g.*, INT'L ASSOC. PRIV. PROS., GLOBAL COMPREHENSIVE PRIVACY LAW MAPPING CHART (2022), https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf [https://perma.cc/2ZES-LQ6K].

Brazil enacted its General Data Protection Law,[12] which broadly aligns with the GDPR, in September 2020.[13] China's Private Information Protection Law,[14] enacted in 2021, is also modeled after the GDPR, but it only regulates private parties.[15] Indonesia and Oman joined the ranks of countries with data protection laws in 2022, to name only two, and more countries are expected to follow the trend in 2023.[16]

The United States shares the growing international concern about consumer data privacy. At the federal level, the Federal Trade Commission (FTC) issued an advanced notice of proposed rulemaking on commercial surveillance and data security, seeking input on "whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."[17] Congress also came the closest it had ever come to passing comprehensive federal privacy legislation[18] when the American Data Privacy and Protection Act ("ADPPA")[19] advanced to the House floor. However, the bill ultimately did not

12. Brazilian General Data Protection Law (LGPD) (as amended by Law No. 13,853/2019), https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf [https://perma.cc/XU9D-MS6P].

13. *Id.*; *see also Compare Data Protection Laws Around the World*, DLA PIPER: DATA PROT. L. OF WORLD, https://www.dlapiperdataprotection.com/index.html [https://perma.cc/368T-7QDH].

14. Roger Creemers & Graham Webster, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DIGICHINA (Sept. 7, 2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021 [https://perma.cc/V2DH-MPBJ].

15. *See* Anupam Chander, *Convergence and Divergence in Global Data Privacy Law: Comparing the GDPR, PIPL, and CCPA, in* PROSPECTS FOR HARMONIZATION OF GLOBAL DATA GOVERNANCE 78, 78 (CENTRE ON REGUL. IN EUR. 2022), https://cerre.eu/wp-content/uploads/2022/11/GGDE_FullReport.pdf [https://perma.cc/7LQP-G4F9].

16. *About*, DLA PIPER: DATA PROT. L. OF WORLD, https://www.dlapiperdataprotection.com/index.html?t=about&c=AL [https://perma.cc/QSL2-8PSJ]. For example, India and Egypt are expected to enact data protection laws in 2023. *Id.*

17. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022).

18. *American Data Privacy and Protection Act*, INT'L ASSOC. PRIV. PROS., https://iapp.org/resources/topics/adppa [https://perma.cc/Z992-GNEM].

19. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

pass due to its provisions that would have preempted more protective state laws like California's Consumer Privacy Act.[20]

State legislatures have also been actively considering and enacting consumer privacy regulations. In 2022, twenty-nine states considered sixty comprehensive privacy bills—an increase of 106 percent over 2021.[21] That momentum has carried into 2023—so far, at least fifteen states have introduced legislation to expand privacy protections.[22] Among enacted and proposed state consumer privacy legislation, two approaches have emerged. The dominant approach has been the Rights /Obligations Model, in which laws grant consumers certain affirmative rights and impose an enumerated list of obligations on businesses.[23] In 2022, Utah and Connecticut passed new consumer privacy laws based on the Rights/Obligations Model, joining California, Colorado, and Virginia as the first five states to enact such laws.[24] The trend shows no signs of slowing; as of September 2023, Delaware, Iowa, Indiana, Montana, Oregon, Tennessee, and Texas have passed similar privacy laws that take the same approach.[25] An emerging trend in these states has

20. Cameron F. Kerry, *Will California Be the Death of National Privacy Legislation?*, BROOKINGS (Nov. 18, 2022), https://www.brookings.edu/blog/techtank/2022/11/18/will-california-be-the-death-of-national-privacy-legislation [https://perma.cc/UB5P-CTB7]; *see also* CAL. CIV. CODE §§ 1789.100–1798.199.100 (2022).

21. *Privacy Matters in the US States*, INT'L ASSOC. PRIV. PROS., https://iapp.org/media/pdf/resource_center/infographic_privacy_matters_in_the_us_states.pdf [https://perma.cc/3NBY-UZFA]. In 2021, only twenty-nine comprehensive consumer privacy bills were considered. *Id.*

22. *See* Christiano Lima, *States Are Readying a Flurry of Privacy Bills as Washington Stalls*, WASH. POST (Jan. 20, 2023), https://www.washingtonpost.com/politics/2023/01/20/states-are-readying-flurry-privacy-bills-washington-stalls [https://perma.cc/LC2K-JG5R]; *see also* CAL. CIV. CODE §§ 1789.100–1798.199.100 (2022); COLO. REV. STAT. § 6-1-1301 (2022); Personal Data Privacy and Online Monitoring Act, S.B. 6, Gen. Assemb., Reg. Sess. (Conn. 2022); Indiana Consumer Data Protection Act, S.B. 0005,5 123d Gen. Assemb., Reg. Sess. (Ind. 2023); 2023 UTAH CODE ANN. § 13-61-101 (2023); VA. CODE ANN. § 59.1-575 (2022).

23. *See infra* Section I.B.; *see also* Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 23–30 (2021) (describing the "second wave" in privacy law as a shift from notice and choice to compliance and rights of control).

24. *See* Anokhy Desai, *US State Privacy Legislation Tracker*, INT'L ASSOC. PRIV. PROFS. (last updated July 7, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/5CJX-JEHC].

25. H.B. 154, 152nd Gen. Assemb., Reg. Sess. (Del. 2023); S.F. 262, 90th Gen. Assemb., Reg. Sess. (Iowa 2023); S.B. 0005, 123d Gen. Assemb., Reg. Sess. (Ind. 2023); H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023); S.B. 384, 68th Leg., Reg. Sess. (Mont. 2023); S.B. 619, 82nd Leg. Assemb., Reg. Sess. (Or. 2023); H.B. 4, 88th Leg. Gen. Assemb. Reg. Sess. (Tex. 2023). At the time of publication, Delaware was the most recent state to pass a comprehensive consumer privacy law. For up-to-date information about the status of state privacy laws, see Desai, *supra* note 24.

been to borrow GDPR terminology. Specifically, every state (except California) uses the terms "data controller" and "data processor" in their consumer privacy laws to determine the extent of the obligations imposed on businesses.[26]

While the enactment of state laws based on the Rights /Obligations Model is an important step forward for consumer privacy protection, there are still gaps in the privacy protection they afford to consumers. For example, most of these laws are business friendly, with carve-outs for targeted advertising.[27] The laws also fail to provide a private right of action or address common problems stemming from intangible privacy harms.[28] As such, lawmakers and scholars continue to consider other ways to safeguard consumer privacy.

Another popular—and divisive—approach working its way into proposed legislation is the Fiduciary Model, inspired by Jack Balkin's Information Fiduciary theory and expanded upon in other scholarly literature.[29] The Fiduciary Model of privacy, which imposes limited fiduciary duties on businesses to their data subjects, has the potential to address the gaps in the Rights /Obligation Model.[30] However, the Fiduciary Model comes with its own drawbacks, as made apparent by legislators' limited attempts to codify various elements of the Fiduciary Model. For example, the 2018 Data Care Act[31] proposed imposing information fiduciary duties on all online service providers, but it would have allowed the FTC to carve out exemptions based on the size of the provider, the nature of the provider's activities, and the sensitivity of consumer information handled by the providers.[32] The 2022 ADPPA included a "duty of loyalty" that would apply to "covered entities," defined broadly as anyone who determines the purposes and means of collecting, processing, or transferring data in a commercial context.[33] Such vague

26. *See infra* Section I.B.
27. *Id.*
28. *Id.*
29. *See infra* Section II.A.
30. *Id.*
31. Data Care Act of 2018, S. 3744, 115th Cong. (2018).
32. *Id.* § 3(d). The Act defines "online service provider" as "an entity that—(A) is engaged in interstate commerce over the internet or any other digital network; and (B) in the course of business, collects individual identifying data about end users, including in a manner that is incidental to the business conducted." *Id.* § 2(4).
33. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(9) (2022).

statutory commands, as exemplified in the Data Care Act and the ADPPA, still leave open questions as to who, exactly, should be subject to fiduciary duties.[34]

In this Article, we argue that borrowing the data controller /data processor distinction from the GDPR and existing U.S. state privacy laws presents a workable path forward for defining data fiduciaries. This analysis proceeds in three parts. Part I discusses the distinction between "data controllers" and "data processors" in the GDPR and how those terms may apply differently in new state consumer privacy laws. Part II analyzes the Fiduciary Model of privacy, highlighting its advantages over the Rights/Obligations Model. It also addresses common critiques of the model. Part III explains how the data controller /data processor distinction is analogous to the theory underlying the Fiduciary Model of privacy, providing a workable definition of "data fiduciaries" in future data privacy legislation. Part III then fills in further gaps in how such consumer privacy laws should be interpreted by arguing that businesses subject to such laws should be considered "data controllers" by default and bear the burden of rebutting that presumption.

I. DATA CONTROLLERS AND DATA PROCESSORS: DEFINITIONS AND SCOPE

The distinction between data controllers and data processors is a key distinction in the GDPR; however, the terms have been interpreted broadly by European courts such that entities are far more likely to be considered controllers than processors. Understanding the European interpretation of the terms is crucial as U.S. states have begun to incorporate the "data controller" and "data processor" distinction into their own consumer privacy laws.[35] This Part will analyze the meaning of "data controller" and "data processor" under European law and

34. However, at the state level, in 2019, 2021, and most recently in February 2023, the New York Senate introduced a bill that would impose limited duties of loyalty and care on "data controllers" and a duty of confidentiality on "data processors." New York Privacy Act, S.B. A3593, Gen. Assemb., 2023–2024 Reg. Sess. (referred to Assemb. Consumer Aff. And Prot. Comm., Feb. 3, 2023).

35. *See, e.g.*, COLO. REV. STAT. §§ 6-1-1303(7), (19) (2022); Personal Data Privacy and Online Monitoring Act, S.B. 6, Gen. Assemb., Reg. Sess. 2022 Conn. Acts. No. 22-15 §§ 1(8), (21); VA. CODE ANN. § 59.1-575 (2022); Senate File 262, 90th Gen. Assemb., Reg. Sess. §§ 1(8), (21) (Iowa 2023); UTAH CODE ANN. §§ 13-61-101(12), (26).

then examine the context in which new U.S. state laws use the terms.

A. Data Controllers and Data Processors in the GDPR

The GDPR, which went into effect in May 2018, is an EU data protection regime that "offers protections that follow the data and imposes data governance duties on companies regardless of whether individuals invoke their rights."[36] There are no threshold requirements that companies must meet in order for the GDPR to take effect, such as number of employees or amount of revenue.[37] Any company with personnel or offices in the European Union is subject to the GDPR.[38] The GDPR also applies to companies with no physical presence in the European Union that offer goods and services (even free ones) to Europeans, provided the company does something more than simply make a website available to show they are offering services to "data subjects"[39] in the European Union.[40] In addition, the GDPR protects any "data subject" physically in the European Union, regardless of their citizenship.[41]

The GDPR's scope is limited by exempting activities for a "purely personal or household activity . . . with no connection to a professional or commercial activity," such as "correspondence and the holding of address or social networking."[42] However, this is a rather narrow exception. For example, the Court of Justice of the European Union ("CJEU") has held that a video camera attached to a home to record the surroundings of the house for the purpose of identifying burglars was not a "purely

36. Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 96 (2020). For more background on the GDPR, see generally *id.*; Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMS. TECH. L.J. 65 (2019).

37. Hoofnagle et al., *supra* note 36, at 74.

38. *Id.*; Jones & Kaminski, *supra* note 36, at 113.

39. A "data subject" is any "identified or identifiable natural person." *See* GDPR, *supra* note 10, at art. 4(1).

40. Hoofnagle et al., *supra* note 36, at 74. For example, using local language or currency on a website might show that the company is offering services to Europeans. *Id.*

41. *Id.* For more information on the jurisdictional scope of the GDPR, *see, e.g.*, Hoofnagle et al., *supra* note 36,. at 73–76; Jones & Kaminski, *supra* note 36, at 112–14.

42. GDPR, *supra* note 10, at Recital 18, art. 2(2)(c).

personal or household activity," thus making the homeowners subject to the GDPR.[43]

The GDPR classifies those to whom it applies as either "data controllers" or "data processors," which have different obligations according to their classification.[44] Data controllers have greater obligations than data processors.[45] Therefore, for any person or organization processing[46] personal data, determining whether they are a controller or a processor is a necessary first step in assessing their compliance.[47] The GDPR defines a controller as a "natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[48] A processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[49] Hoofnagle et al. explain how this concept works in simple cases:

> [I]f company Y gathers and analyzes survey data on the customers of company X, as instructed by company X, company X is the controller and company Y the data processor. If two organizations work together in determining why and how personal data will be processed, they will be seen as joint controllers and will share the regulatory burden and liability for errors and mistakes.[50]

Of course, not every case is so simple, and the CJEU's jurisprudence on the matter has expanded the definition of "data controller" to encompass entities that might previously have been considered "data processors." The CJEU has held that no

43. Hoofnagle et al., *supra* note 36, at 75.

44. *See* GDPR, *supra* note 10, at arts. 24–43.

45. *Id.*

46. "'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR art. 4(2).

47. Yordanka Ivanova, *Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World*, *in* PERSONAL DATA PROTECTION AND LEGAL DEVELOPMENTS IN THE EUROPEAN UNION 1 (M. Tzanou ed., 2020)*; see also* Jones & Kaminski, *supra* note 36, at 115.

48. GDPR, *supra* note 10, at art. 4(7).

49. *Id.* at art. 4(8).

50. Hoofnagle et al., *supra* note 36, at 73.

actual access to personal data is required for a person or entity to be categorized as a controller.[51] For example, the CJEU held that the administrator of a Facebook fan page—who does not actually access or control any personal data of the fan page's members—is still a data controller per the GDPR because they played a role in determining the purposes and means in which Facebook processed data by "defining the type of statistics and the objectives of managing and promoting its activities."[52] The CJEU also found that a company that embedded the Facebook "like" plug-in on its website was a data controller because, "by simply choosing to integrate a third party service processing personal data, the website operator 'exerts a decisive influence over the collection and transmission of the personal data of visitors to that website' to the third party service provider . . . ."'[53] Because personal data would not have been collected and transmitted to a third party (Facebook) without the website operator's choice to embed a "like" button, the website operator determined the "means" of collecting and processing data, thus making the operator a data controller.[54]

Data controllers can also be "joint controllers."[55] The CJEU's interpretation of joint controllership has further expanded the data controller category. For example, CJEU case law indicates that two or more parties are joint controllers when "they are pursuing a common purpose, a purpose of their own, or have some legitimate interest (economic or other) in the processing of the personal data."[56] In the Facebook example discussed previously, the company that embedded the Facebook "like" button on its website would be considered a joint controller alongside Facebook.[57]

While the CJEU interprets "data controller" broadly, it construes "data processor" much more narrowly. Generally, a person or entity is a processor if their activity is delegated to

51. *See* Case C-131/12, Google Spain v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317, ¶¶ 34, 38 (May 13, 2014); Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Facebook Fanpage) v.Wirtschaftsakademie Schleswig-Holstein GmbH, EU:C:2018:388, ¶ 28 (June 5, 2018)*; see also* Ivanova, *supra* note 47, at 4.

52. Ivanova, *supra* note 47, at 5; Facebook Fanpage, Case C-210/16 at ¶ 28.

53. Ivanova, *supra* note 47, at 5 (quoting Case C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629 (July 29, 2019)).

54. *Id.*

55. *See* GDPR, *supra* note 10, at art. 4(7); Hoofnagle et al., *supra* note 36, at 73.

56. Ivanova, *supra* note 47, at 6.

57. Facebook Fanpage, Case C-210/16 at ¶¶ 35–39.

them from a controller.[58] The delegation can be limited to a specific task or context, or it can be more general.[59] Additionally, a contract is needed to specify the matter of delegation and the processor's obligations.[60] The processor must "act only on instructions and under the control of the service provider" within that contract.[61] As such, the concept of a "data processor" seems to be of limited practical application.[62] Circumstances that may suggest an entity is a processor include the amount of instruction given by the controller, the degree of monitoring and supervision by the controller in the processing of the data, and the expertise of the service provider.[63] Data processors have fewer obligations than data controllers under the GDPR—their primary obligation being to process the data according to the controller's instructions.[64] Controllers, on the other hand, are subject to a variety of obligations, such as recordkeeping, developing a data protection plan, appointing a Data Protection Officer, and incorporating data protection by design.[65]

While the distinction between controllers and processors is crucial for entities seeking to comply with the GDPR, current CJEU jurisprudence indicates that the data controller category is nearly all-encompassing. However, some key points can be extrapolated. Taken together, CJEU case law suggests that a "data controller" per the GDPR is an entity that (1) has access to a user's personal data—either directly or through an intermediary; (2) has a commercial interest in a user's personal data; and (3) exerts influence over the processing of personal information—including collection, transmission, storage, and analysis of such data.[66] On the other hand, data processors generally have clear contractual guidelines determined by the

58. *See* Ivanova, *supra* note at 47, at 7–8.

59. *See id.*

60. GDPR, *supra* note 10, at art. 28(3).

61. Ivanova, *supra* note 47, at 7–8 (quoting Case C-119/12, Josef Probst v mr.nexnet GmbH, ECLI:EU:C:2012:748, ¶¶ 40–47 (Nov. 22, 2012)).

62. *See id.*; *see also* Mike Hintze, *Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR*, J. INTERNET L., 17, 18–19 (2018) (discussing ambiguities in distinguishing between data controllers and data processors).

63. *See* Ivanova, *supra* note 47, at 8.

64. *Id.* at 13.

65. GDPR, *supra* note 10, at art. 24–43. For more information about the duties of data controllers and processors, see Hoofnagle et al., *supra* note 36, at 85–88.

66. *See supra* notes 48–63 and accompanying text.

data controller; any degree of influence over the processing of personal information is likely to make a would-be data processor a "joint controller" instead.[67]

B. Data Controllers and Data Processors in U.S. State Law

The European Union's broad interpretation of data controllers is important to keep in mind as several U.S. states have incorporated the same terms, with the same definitions, into their newly enacted consumer privacy laws based on the Rights/Obligations Model. Thus far, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia have passed similar consumer privacy laws that use nearly identical definitions of "controller" and "processor" to the GDPR.[68]

67. *See supra* notes 55–63 and accompanying text.

68. *Compare* GDPR, *supra* note 10, at art. 4(7)–(8) (defining data controller and data processor) *with* COLO. REV. STAT. §§ 6-1-1303(7), (19) (2023) (using the same definitions); Personal Data Privacy and Online Monitoring Act, 2022 Conn. Acts. No. 22-15 §§ 1(8), (21) (same); VA. CODE ANN. § 59.1-575 (2023) (same); S.B. 262, 90th Gen. Assemb., Reg. Sess. §§ 1(8), (21) (Iowa 2023) (same); Indiana Consumer Data Protection Act, S.B. 0005, 123d Gen. Assemb., Reg. Sess. §§ 2(9), (22) (Ind. 2023) (same); Tennessee Information Protection Act, H.B. 1181, 113th Gen. Assemb., Reg. Sess. §§ 2(8), (20) (Tenn. 2023); Montana Consumer Data Privacy Act, S.B. 384, 68th Gen. Assemb., Reg. Sess. §§ 2(8), (18) (Mont. 2023); Texas Data Privacy and Security Act, H.B. 4, 88th Gen. Assemb. Reg. Sess. §§ 2(8), (23) (Tex. 2023); Delaware Personal Data Privacy Act, H.B. 154, 152nd Gen. Assemb. §§ 1(9), (24) (Del. 2023) (same); Oregon Consumer Privacy Act, S.B. 619, 82nd Gen. Assemb., Reg. Sess. §§ 1(8), (15) (Or. 2023) (same); UTAH CODE ANN. §§ 13-61-101(12), (26) (2023) (using the same definition of "processor" and a slightly altered definition of "controller"). *See infra* Tables 1 & 2.

Table 1: Data Controller—Legal Definitions

Law	Jurisdiction	Definition
GDPR	European Union	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Colorado Privacy Act	Colorado	A person that, alone or jointly with others, determines the purposes for and means of processing personal data.
Connecticut Data Privacy Act	Connecticut	An individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.
Delaware Personal Data Privacy Act	Delaware	A person that, alone or jointly with others, determines the purpose and means of processing personal data.
Indiana Consumer Data Protection Act	Indiana	A person that, alone or jointly with others, determines the purpose and means of processing personal data.
Iowa Consumer Data Protection Act	Iowa	A person that, alone or jointly with others, determines the purpose and means of processing personal data.

Montana Consumer Data Privacy Act	Montana	An individual who or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data.
Oregon Consumer Privacy Act	Oregon	A person that, alone or jointly with another person, determines the purposes and means for processing personal data.
Tennessee Information Protection Act	Tennessee	The natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal information.
Texas Data Privacy and Security Act	Texas	An individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data.
Utah Consumer Privacy Act	Utah	A person doing business in the state who determines the purposes for which and the means by which personal data are processed, regardless of whether the person makes the determination alone or with others.
Virginia Consumer Data Protection Act	Virginia	The natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

Table 2: Data Processor—Legal Definitions

Law	Jurisdiction	Definition
GDPR	European Union	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Colorado Privacy Act	Colorado	A person that processes personal data on behalf of a controller.
Connecticut Data Privacy Act	Connecticut	An individual who, or legal entity that, processes personal data on behalf of a controller.
Delaware Personal Data Privacy Act	Delaware	A person that processes personal data on behalf of a controller.
Indiana Consumer Data Protection Act	Indiana	A person that processes personal data on behalf of a controller.
Iowa Consumer Data Protection Act	Iowa	A person that processes personal data on behalf of a controller.
Montana Consumer Data Privacy Act	Montana	An individual who or legal entity that processes personal data on behalf of a controller.
Oregon Consumer Privacy Act	Oregon	A person that processes personal data on behalf of a controller.

Tennessee Information Protection Act	Tennessee	A natural or legal entity that processes personal information on behalf of a controller.
Texas Data Privacy and Security Act	Texas	A person that processes personal data on behalf of a controller.
Utah Consumer Privacy Act	Utah	A person who processes personal data on behalf of a controller.
Virginia Consumer Data Protection Act	Virginia	A natural or legal entity that processes personal data on behalf of a controller.

Although the definitions of controller and processor are nearly identical across jurisdictions,[69] as shown in Tables 1 and 2 above, the controller and processor terms do not apply to as many entities under U.S. law as they do under the GDPR. All of the above U.S. laws limit their application to businesses that meet certain revenue or customer thresholds, thus limiting their scope.[70] Yet despite differences in scope between the GDPR and U.S. state laws, the virtually identical terms and definitions

69. One exception is the Florida Digital Bill of Rights, enacted in June 2023. 2023 FLA. LAWS 2023-201. Florida's privacy law imposes many of the same obligations on data controllers, along with a few unique obligations, but it has a much narrower definition of "data controllers" than other state privacy laws that significantly limits its scope. *See id.* § 501.702(9). Under Florida's law, a "data controller" is an entity that (1) "determines the purposes and means of processing personal data about consumers alone or jointly with others," (2) generates more than $1 billion in annual global revenue, and (3) meets at least one of the following criteria: derives at least fifty percent of its global annual revenues "from the sale of advertisements online, including providing targeted advertising or the sale of ads online;" "operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation;" or "operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install." *Id.*

70. For a comparison of the scope of existing laws see INT'L ASSOC. PRIV. PROS., US STATE COMPREHENSIVE PRIVACY LAWS: 2022 LEGISLATIVE SESSION 8 (2023), https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_overview.pdf [https://perma.cc/G3Q2-V2D3] (comparing the scope of existing laws).

suggest that interpretations of these terms within the scope of new U.S. state laws may be influenced by CJEU jurisprudence.

Another commonality between these state laws is that they are all modeled after the proposed Washington Privacy Act.[71] Although the Washington Privacy Act was never passed, it has had a notable influence on privacy legislation in other states.[72] The history of this Act has been traced back to Microsoft and the "Brussels Effect"[73] because Microsoft promoted the Act in accordance with its preference for privacy legislation that is similar to the GDPR. Because Microsoft already must comply with the GDPR, U.S. state privacy legislation that is closely aligned with the GDPR would simplify compliance and save the company money.[74] Despite the failure of the bill in Washington, several other states have enacted similar laws with those definitions—and more will likely follow suit.[75] As these terms become common, it is even more important to have a clear understanding of data controllers and data processors. It is also important to recognize the shortcomings of the Rights /Obligations Model and its implementation in these statutes as a majority of states continue to debate whether and how to implement consumer privacy regulation.

While any consumer privacy regulation is a step in the right direction, existing state laws leave gaps where consumers are left unprotected. To begin with, California is the only state to create a private right of action, meaning that in the other states listed in the tables above, enforcement will be dependent on the attorneys general.[76] This is especially problematic for people from marginalized communities who generally "have not been able to count on government institutions to vindicate their

71. S. 5376, 66th Leg., Reg. Sess. (Wash. 2019). The Washington Privacy Act has narrowly failed to become law twice. *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1788 (2021); J. SCOTT BABWAH BRENNEN & MATT PERAULT, UNIV. OF N.C. CTR. ON TECH. POL'Y, THE STATE OF STATE PLATFORM REGULATION 8 (2022).

72. *See* Chander et al., *supra* note 71, at 1788.

73. *See infra* Section III.A.

74. Chander et al., *supra* note 71, at 1788–89.

75. COLO. REV. STAT. § 6-1-1301 (2023); Personal Data Privacy and Online Monitoring Act, 2022 Conn. Acts. No. 22-15; UTAH CODE ANN. § 13-61-101 (2023); VA. CODE ANN. § 59.1-575 (2023); Senate Bill 262, 90th Gen. Assemb., Reg. Sess. (Iowa 2023); S.B. 0005, 123rd Gen. Assemb., Reg. Sess. (Ind. 2023); H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023); S.B. 384, 68th Leg., Reg. Sess. (Mont. 2023).

76. *See* CAL CIV. CODE § 1798.150(a)(1) (2023).

rights."[77] A private right of action—even a limited one, as in California[78]—would "guarantee that those who could be most negatively impacted by bad corporate practices could have any form of redress."[79] But even with a private right of action, it is unclear whether the rights or obligations in these state laws, if violated, would give rise to an injury that courts would deem sufficiently cognizable to grant plaintiffs standing—a common problem in privacy litigation.[80]

In addition to insufficient enforcement mechanisms, the Rights/Obligations Model also allows states to limit consumer rights and obligations in a way that means geography could ultimately determine an individual's basic privacy rights.[81] Utah's and Virginia's consumer privacy laws, for example, do not include provisions on "dark patterns" or require data protection assessments.[82] In addition, there are gaps in the enumerated rights in many states' laws, leaving consumers unprotected from targeted advertising and unforeseeable future uses of

77. Joseph Duball, *Colorado Privacy Act Passes, Professionals Ponder Effects*, INT'L ASSOC. PRIV. PROS. (June 9, 2021), https://iapp.org/news/a/colorado-privacy-act-passes-professionals-ponder-effects [https://perma.cc/QKF3-M4TV].

78. *See* CAL CIV. CODE § 1798.150(a)(1) (2023); *see also* Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, INT'L ASSOC. PRIV. PROS. (June 8, 2020), https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action [https://perma.cc/A9ZZ-9UPM].

79. Duball (2021), *supra* note 77 (quoting Silicon Flatirons Executive Director Amie Stepanovich); *see also* Becky Chao, Eric Null & Claire Park, *A Private Right of Action Is Key to Ensuring the Consumers Have Their Own Avenue for Redress*, *Enforcing a New Privacy Law*, NEW AMERICA (Nov. 20, 2019), https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress [https://perma.cc/GM3N-5D6W] (discussing the importance of a private right of action in privacy laws).

80. *See, e.g.*, Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez*,* 101 B.U. L. REV. ONLINE 62, *passim* (2021); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 816–19 (2022).

81. *See* Citron & Solove, *supra* note 80, at 807; Keir Lamont, *Utah Consumer Privacy Act Passes State Legislature*, FUTURE OF PRIV. F. (Mar. 4, 2022), https://fpf.org/blog/utah-consumer-privacy-act-passes-state-legislature [https://perma.cc/8STW-8W4B]. The Utah Consumer Privacy Act sets "significantly narrower individual rights and business obligations than privacy regimes enacted in other states." *Id.*

82. Joseph Duball, *Utah on the Cusp of US's Latest Comprehensive State Privacy Law*, INT'L ASSOC. PRIV. PROS. (Mar. 3, 2022), https://iapp.org/news/a/utah-on-the-cusp-of-uss-latest-comprehensive-state-privacy-law [https://perma.cc/HBP6-DTHZ].

aggregated personal data.[83] Virginia's law, for example, carves out language that allows businesses to continue some targeted advertising practices even if consumers opt out.[84] And Iowa's recently enacted privacy law has been described as a "wish list of industry-sought provisions" that excludes several rights and obligations that other states have opted to include.[85] Thus, there are still gaps in the trending Rights/Obligations Model of privacy that must be addressed to ensure consistent consumer privacy protection in U.S. law.

II. THE PROMISE AND PERIL OF THE FIDUCIARY MODEL OF PRIVACY

The Fiduciary Model presents a solution to fill the gaps in the Rights/Obligations Model. This Part proceeds in three sections. Section A briefly describes the origins and functions of the Fiduciary Model. Section B highlights the promise of the Fiduciary Model to better protect consumer privacy. Finally, Section C addresses the model's common critiques.

A. The Origins of the Fiduciary Model

Federal and state law have long recognized special fiduciary relationships in which the fiduciary has "special obligations of loyalty and trustworthiness toward [the beneficiary]" and

83. Duball (2021), *supra* note 77; David Stauss & Stacey Weber, *How do the CPRA, CPA & VCDPA Treat Dark Patterns?*, HUSCH BLACKWELL: BYTE BACK (Mar. 16, 2022), https://www.bytebacklaw.com/2022/03/how-do-the-cpra-cpa-and-vcdpa-treat-dark-pattern [https://perma.cc/733W-AYAN] (noting that Virginia's privacy law does not address dark patterns); *see also* UTAH CODE ANN. § 13-61-101 (2023); VA. CODE ANN. § 59.1-575 (2022).

84. Christopher Escobedo Hart & Colin Zick, *Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection*, JD SUPRA (July 7, 2021), https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636 [https://perma.cc/254S-FFH3].

85. *See* Joseph Duball, *Iowa Set to Finalize Sixth US Comprehensive State Privacy Law*, INT'L ASSOC. PRIV. PROS. (Mar. 16, 2022), https://iapp.org/news/a/iowa-set-to-finalize-sixth-us-comprehensive-state-privacy-law [https://perma.cc/2JNK-9WB6] (noting that Iowa's privacy law does not include data protection assessments, the ability to opt out of targeted advertising, sensitive data opt-in consent, or a user's right to correct, among other deficiencies). For a list of rights and obligations featured in enacted and proposed state statutes, see *US State Privacy Legislation Tracker*, INT'L ASSOC. PRIV. PROS. (July 7, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/9QRP-LGF3].

therefore must act in the beneficiary's best interest.[86] Traditional fiduciary relationships include doctor-patient and attorney-client relationships.[87] Jack Balkin argues that "the explosion of the collection and use of personal data" in the digital age has created a new category of fiduciary relationships: information fiduciaries.[88] Like traditional fiduciary relationships, Balkin argues that information fiduciary relationships occur when there are asymmetries in power and information between online service providers ("OSPs") and their users.[89] He sums up the problem nicely: "By presenting themselves as trustworthy collectors and keepers of our individual data, and by emphasizing that, for reasons of security and competitiveness, they cannot be fully transparent, digital organizations induce relations of trust from us, so that we will continue to use their services."[90] For that reason, Balkin argues, certain OSPs should be classified as information fiduciaries.[91]

Which OSPs, exactly? Balkin defines an information fiduciary broadly as "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."[92] People and companies act as information fiduciaries when three conditions are met: (1) they hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them; (2) they give users a reason to believe they will not misuse or disclose their personal information; and (3) the users reasonably believe these companies will not disclose or misuse their data.[93] While charged with special duties, information fiduciaries should not be held to the same standards as traditional fiduciaries under

86. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1207 (2016) [hereinafter Balkin, *Information Fiduciaries*]; *see also* RICHARD T. OSTLUND & DAN HALL, BUSINESS AND COMMERCIAL LITIGATION IN FEDERAL COURTS § 136:2 (5th ed. 2021) ("Typically, in the absence of federal statutory preemption, fiduciary duty claims are governed by state law.").

87. Balkin, *Information Fiduciaries*, *supra* note 86, at 1209.

88. *Id.* at 1221.

89. *Id.* at 1222.

90. *Id.* at 1223.

91. *Id.*

92. *Id.* at 1209.

93. *Id.* at 1223–24.

Balkin's framework.[94] This is because OSPs, like Facebook, do not perform the same kinds of services—or collect the same kinds or volume of information—as traditional fiduciaries like doctors or lawyers.[95] Instead, he proposes three basic duties information fiduciaries have to their users. The first two duties are the duty of care and the duty of loyalty, which function similarly to the duties of care and loyalty in the general fiduciary context.[96] He also proposes a third duty: the duty of confidentiality, which functions alongside the duty of care to require OSPs to keep their customers' data confidential and secure.[97] Balkin argues these duties should "run with the data," meaning that the original data collector is responsible for keeping its users' data secure.[98]

Other scholars have built upon this model, theorizing about variations of information-fiduciary-esque duties in various contexts with different triggers, remedies, and enforcement mechanisms.[99] For example, scholars have suggested that duties should be triggered by default in all consumer transactions,[100] that they should be triggered when companies abuse users' trust,[101] or that they should only be triggered by agreement from both parties.[102] Neil Richards and Woodrow Hartzog argue that data collectors should owe their users a duty

94. Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 14–15 (2020) [hereinafter Balkin, *Fiduciary Model*]; Jack M. Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011, 2051 (2018) [hereinafter Balkin, *Free Speech*].

95. Balkin, *Fiduciary Model*, *supra* note 94, at 14–15; *see* Balkin, *Free Speech*, *supra* note 94, at 2051.

96. Balkin, *Fiduciary Model*, *supra* note 94, at 14.

97. *Id.*

98. Balkin, *Free Speech*, *supra* note 94, at 2051.

99. *See, e.g.*, Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches,* 127 YALE L.J. F. 614, 625–26 (2018); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1 (2018); Harold Feld, *Privacy Legislation, Not Common Law Duties*, LPE PROJECT (July 4, 2019), https://lpeproject.org/blog/privacy-legislation-not-common-law-duties [https://perma.cc/M3BS-W6UP]; Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 IOWA J. CORP. L. 143 (2020).

100. *See, e.g.*, Barrett, *supra* note 99, at 1092–94; Scholz, *supra* note 99, at 187–91 (2020).

101. Dobkin, *supra* note 99, at 7, 17.

102. Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Care and Loyalty in the Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75, 102–17 (2019).

of loyalty whenever there is an information relationship between a user and a data collector—essentially, whenever personal information is disclosed to an organization.[103] This version of a duty of loyalty functionally incorporates the duty of confidentiality from Balkin's model.[104] Scholars have also proposed various duties in the context of data security[105] and the Fourth Amendment.[106] Table 3 below highlights some of the scholarly interpretations and extensions of the Fiduciary Model of privacy, illustrating the different definitions and triggers scholars have proposed.

Table 3: Summary of Scholars' Approaches to the Fiduciary Model

Scholar(s)	Theory Label	Definition	When Duty Triggered
Jack Balkin	Information Fiduciary	"A person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."	Three conditions must be met by a person or company ("online service provider"): (1) they hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them; (2) they give users a

103. *See* Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 371, 378–79 (2022) [hereinafter Hartzog & Richards, *Legislating*].

104. *See* Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 1024–32 (2022) [hereinafter Hartzog & Richards, *Surprising Virtues*].

105. *See generally* Solow-Niederman, *supra* note 99; William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (2019).

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

			reason to believe they will not misuse or disclose their personal information; and (3) the users reasonably believe these companies will not disclose or misuse their data based on existing social norms or patterns of practice.
Woodrow Hartzog & Neil Richards	Duty of Loyalty	The duty of data collectors to act in the best interests of those whose data they collect.	When there is an information relationship; when personal information is disclosed to an organization.
Alicia Solow-Niederman	Data Confidant	Data confidants have a duty to securely maintain the information that they receive from customers.	If a similarly situated consumer would disclose data only if they reasonably understood there to be an implicit or explicit guarantee of confidentiality.
Richard S. Whitt	Digital Trustmediary ("DTM")	The DTM model involves entities providing advanced digital service to their clients, while	Voluntary agreement by both parties.

		voluntarily operating under heightened fiduciary duties of loyalty, care, and confidentiality.	
Lindsey Barrett	Information Fiduciary	Same as Balkin.	Compulsory for all data collectors.
Lauren Scholz	Fiduciary Boilerplate	Technology-neutral protections for consumers against exploitation.	Implied in all consumer transactions as a matter of law.
Ariel Dobkin	Information Fiduciary	Same as Balkin.	Companies breach the fiduciary duty when they abuse users' trust by: (1) using their data to manipulate them; (2) using their data to discriminate against them; (3) sharing their data with third parties without consent; or (4) violating their own privacy policies.
Kiel Brennan-Marquez	Fourth Amendment Fiduciaries	Under conditions of practically involuntary, arm's length entrustment, one should be	When the counterparty (the information holder) has such power over the data subject

		able to expect that shared information will be used only for limited purposes and certainly not to expose one to criminal liability.	that worries about opportunism and susceptibility to abuse arise.

B. The Promise: How the Data Fiduciary Model Improves on Existing State Consumer Privacy Laws

The Fiduciary Model of privacy has caught the attention of scholars and lawmakers for several important reasons: the model helps circumvent barriers to litigation in federal courts, creates duties that will withstand changes in technology, and circumvents some First Amendment challenges present in many privacy laws. First, because the Fiduciary Model of privacy focuses broadly on the relationship between platforms and the people who use them, an information fiduciary law can circumvent barriers to privacy litigation in federal courts that many other privacy litigants have struggled with, such as standing and causation.[107] One core strength of the Fiduciary Model is its grounding in preexisting fiduciary principles. Courts have long acknowledged in the traditional fiduciary context that the harms that stem from a breach of fiduciary duties are sufficient grounds to establish standing.[108] By imposing analogous duties in the data privacy context, courts may also be more willing to recognize harms that stem from the breach of data fiduciary duties as cognizable.[109] In addition, because the Fiduciary Model is grounded in traditional fiduciary theory, there is room for data fiduciary duties to function as a common law remedy for consumer privacy harms, even if a statute does not create a private right of action.[110]

The Fiduciary Model also creates duties that are future-proof, in that they are flexible enough to hold up to continuous

107. Hartzog & Richards, *Surprising Virtues*, *supra* note 104, at 1004.
108. *Id.*
109. *See id.*
110. *See, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 86, at 1225; Scholz, *supra* note 99, at 145.

changes in technology. Rather than regulating particular activities, the duties of loyalty, confidentiality, and care—or any subset of the three—allow regulators to redefine what it means to fulfill those duties as technology continues to develop.[111] Further, the data fiduciary duties can reach further than the existing Rights/Obligation Model. For example, information fiduciary duties could mitigate issues that arise from microtargeted political ads on platforms like Facebook that rely on hyper-specific user data and dark patterns to target advertisements.[112] In addition to future-proofing, this flexibility also prevents carve-outs for business practices like targeted advertising that businesses have successfully lobbied for in laws grounded in the Rights/Obligations Model.[113]

Finally, proponents of the Fiduciary Model of privacy argue that the model can circumvent concerns that arise at the intersection of data privacy regulation and the First Amendment.[114] A common response to many attempts to regulate data privacy is that data is speech, and thus the way companies use their data is subject to the highest level of First Amendment protection.[115] Balkin's initial proposal of the Fiduciary Model highlighted the fact that fiduciary duties regulate *relationships* rather than pure speech.[116] As Balkin notes, "the First Amendment treats information practices by fiduciaries very differently than it treats information practices involving relative strangers."[117] For example, traditional

111. Hartzog & Richards, *Surprising Virtues*, *supra* note 104, at 1013–15.

112. *See, e.g.*, Kimberly Rhum, Note, *Information Fiduciaries and Political Microtargeting: A Legal Framework for Regulating Political Advertising on Digital Platforms*, 115 NW. U. L. REV. 1829 (2021); Hartzog & Richards, *Surprising Virtues*, *supra* note 104; Jack M. Balkin, *Free Speech in the Algorithmic Society,* 51 U.C. DAVIS L. REV. 1149, 1160–63 (2018) [hereinafter Balkin, *Algorithmic Society*].

113. *See supra* Section I.B.

114. We are mindful of the possible tension between strong data protection laws and the First Amendment. That discussion is beyond the scope of this paper, but we invite future research to address First Amendment considerations. For a general discussion about privacy and the First Amendment, see generally, for example, Neil M. Richards, *Reconciling Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005); Robert C. Post & Jennifer E. Rothman, *The First Amendment and the Right(s) of Publicity*, 130 YALE L. REV. 86 (2020); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501 (2015).

115. *See generally* Balkin, *Information Fiduciaries, supra* note 86; *see also* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014).

116. Balkin, *Information Fiduciaries*, *supra* note 86, at 1209–20.

117. *Id*. at 1209.

fiduciaries (like lawyers and doctors) are prohibited from using clients' sensitive information to their own advantage (or to the client's disadvantage), and this prohibition on such uses does not violate the First Amendment.[118] Relationships between data collectors and their data subjects—like relationships between doctors and patients—do involve speech, but those relationships may be regulated all the same due to the power and information asymmetries between the parties.[119]

C. The Peril: Platform Power, Mixed Loyalties, and Vagueness

Notable privacy scholars have recognized the appeal of the logic underlying Balkin's information fiduciary theory and have built on the idea.[120] However, others are more skeptical of the theory and its offshoots.[121] The main criticisms of the Fiduciary Model entail: (1) the problem of mixed loyalties to shareholders and users; (2) the Fiduciary Model's supposed indifference to platform power; and (3) vagueness.

First, Professor Lina Khan (now FTC Chairwoman) and Professor David Pozen have expressed skepticism about Balkin's theory because they fear firm directors will suffer mixed loyalties.[122] Unlike traditional fiduciaries (like doctors and lawyers), directors of publicly traded firms (like Meta) already owe fiduciary duties to their shareholders, so creating additional fiduciary duties to users would divide firms' loyalties.[123] They argue that, in the event of such a conflict of interest, Delaware law would require companies to act in the best interests of their shareholders before those of their users, and there is no effective

118. *Id.* at 1209–11; *see also* Claudia E. Haupt, *The Limits of Professional Speech*, YALE L.J. F. 185, 191 (2018). *But see* Jane R. Bambauer, *The Relationships Between Speech and Conduct*, 49 U.C. DAVIS L. REV. 1941, 1943–44 (2016) (discussing the implications of a relational approach to free speech and questioning whether Balkin's theory can justify strong confidentiality laws). For a discussion of First Amendment doctrine in the context of professional speech, see generally Rodney Smolla, *Professional Speech and the First Amendment*, 119 W. VA. L. REV. 67 (2016).

119. *See* Balkin, *Information Fiduciaries*, *supra* note 86, at 1214–16.

120. *See supra* notes 99–106 and accompanying text.

121. For other critiques, see generally *Symposia: Information Fiduciaries*, LPE PROJECT, https://lpeproject.org/symposia/information-fiduciaries [https://perma.cc/2XM9-UBGC].

122. Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 508–10 (2019).

123. *Id.*

way to work around this conflict.[124] However, a federal privacy statute that preempts state laws like Delaware's would solve that problem.[125] In addition, other areas of law, like consumer protection, environmental law, and antitrust law also interfere with companies' abilities to maximize profit for their shareholders in every possible way, but shareholders assume the corporations will attempt to comply with the law even if this reduces the shareholders' value.[126]

Another critique, also championed by Khan and Pozen, suggests that the prioritization of the information fiduciary framework, especially regarding online platforms, may come at the expense of increased antitrust enforcement directed at these platforms. They worry that the information fiduciary framework "invites . . . complacency toward online platforms' structural power and a premature abandonment of more robust visions of public regulation."[127] In their opinion, a more effective solution to privacy issues would come from an antitrust approach, limiting the dominance of major online service providers like Meta and Google rather than designing legislation around their dominance.[128] Balkin agrees with Khan and Pozen that the power of large platforms is a structural problem that requires antitrust regulation.[129] However, he argues that the law needs to change in multiple ways to address the problem of large platform power.[130] One necessary intervention, as Khan and Pozen urge, is to take antitrust measures. However, focusing on antitrust regulation alone without also addressing digital privacy will likely exacerbate threats to digital privacy.[131] As James Grimmelmann notes, data fiduciaries are but one tool in the "regulatory toolbox" and will not solve every problem posed by online platforms[132]—but they should not be expected to.

124. *Id.*
125. Balkin, *Fiduciary Model*, *supra* note 94, at 22–23.
126. *Id.*
127. Khan & Pozen, *supra* note 122, at 498.
128. *Id.* at 528. Of course, antitrust regulations may involve sharing more data, which would mean weaker privacy protections. *See* Mark A. Lemley, *The Contradictions of Platform Power*, 1 J. FREE SPEECH L. 303, 311–18 (2021).
129. Balkin, *Fiduciary Model*, *supra* note 94, at 20.
130. *Id.* at 21.
131. *Id.*; *see also* Lemley, *supra* note 128, at 311–18 (explaining how antitrust regulations may increase privacy risks).
132. James Grimmelmann, *When All You Have Is a Fiduciary*, LPE PROJECT (May 30, 2019), https://lpeproject.org/blog/when-all-you-have-is-a-fiduciary [https://perma.cc/R53E-FBQC].

A final concern, noted by Professor Julie Cohen, is whether fiduciary duties can adequately scale to large platforms.[133] Classic fiduciaries (like doctors and lawyers) operate on smaller scales and are built on human-to-human interactions.[134] Because the relationship between people and large platforms is different in scale, speed, and humanity, critics worry that privacy regulation based on duties and principles rooted in trust and loyalty are "too general to be helpful" when it comes to enforcement.[135] Her critique suggests that these duties are aspirational rather than enforceable. In response, Balkin notes that "many existing legal obligations involve vague standards," and those concerns are addressed through common law decision-making or adjudication and rulemaking by administrative agencies.[136] Other scholars have similarly responded to the most prevalent critiques of the Fiduciary Model.[137] For example, Richards and Hartzog address the problem of vagueness in their proposed duty of loyalty. Like fiduciary duties, they argue that such loyalty is superior:

> [It] places the focus for information-age problems where it belongs: not primarily on the data, but on the human relationships that data can affect; not just on procedural requirements for data processing but also on substantive rules restricting dangerous applications; and not merely on the interests of individuals but also on the interests of groups with the same relational vulnerabilities.[138]

Essentially, they argue that the vagueness of loyalty is also a strength, allowing for greater flexibility and adaptability across

133. Julie E. Cohen, *Scaling Trust and Other Fictions*, LPE PROJECT (May 29, 2019), https://lpeproject.org/blog/scaling-trust-and-other-fictions [https://perma.cc/4SU5-7NKB].

134. *Id.*

135. *Id.*; *see, e.g.*, Julie E. Cohen, *How Not to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. 1, 12 (2020); James Grimmelmann, *supra* note 132 (noting that while the information fiduciary model is a good way to conceptualize the privacy interests users have in data held by online platforms, the model is too vague in its current state).

136. Balkin, *Fiduciary Model*, *supra* note 94, at 24.

137. *See generally, e.g.*, Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897 (2021); Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34 (2020).

138. Hartzog & Richards, *Surprising Virtues*, *supra* note 104, at 988–89.

different contexts and cultures.[139] This logic can extend to the other duties of care and confidentiality included in the Fiduciary Model.

In sum, there are compelling strengths and weaknesses inherent in both the Rights/Obligations Model and the Fiduciary Model of privacy. While the Rights/Obligations Model provides greater notice to business about their obligations, it also leaves lots of room for businesses to push for carve-outs to the specified obligations, thus limiting the scope of privacy protection afforded to consumers. In addition, most laws that have followed this model do not create a private right of action—an avenue for legal recourse to ensure consumers can vindicate their interests.[140] The Fiduciary Model creates an opening for recognition of a common law duty that could fill the gap in legislation that omits a private right of action.[141] Recognizing such a duty would also help address the standing problem in privacy litigation.[142] The Fiduciary Model also provides a degree of future-proofing and closes gaps that would allow companies to misuse consumers' data.[143] However, critics have noted that the flexibility of fiduciary duties also makes it harder for consumers and businesses alike to know when those duties have been violated.[144]

Despite critiques, the Fiduciary Model yields strong benefits and protections for consumers. The model provides greater opportunity for consumers with intangible injuries to seek remedies in court, it is future-proof in the face of constantly changing technology, it closes gaps in the Rights/Obligations Model, and it holds up to First Amendment scrutiny. Therefore, we propose harnessing the benefits of the Fiduciary Model and incorporating it into the existing data controller/data processor distinction to create more robust consumer privacy protections that work in harmony with existing state and international law.

139. *See generally, id.* (rebutting critiques of the data loyalty model).

140. *See, e.g.*, COLO. REV. STAT. § 6-1-1301 (2022); Personal Data Privacy and Online Monitoring Act, 2022 Conn. Acts. No. 22-15; UTAH CODE ANN. § 13-61-101; VA. CODE ANN. § 59.1-575 (2022).

141. *See, e.g.*, Balkin, *Fiduciary Model*, *supra* note 94, at 1225; Scholz, *supra* note 99, at 145.

142. *See supra* notes 107–110 and accompanying text.

143. *See* Hartzog & Richards, *Surprising Virtues*, *supra* note 104, at 1013.

144. *See, e.g.*, Cohen (2020), *supra* note 135, at 12.

III. DEVIL'S IN THE DEFINITIONS & DETAILS

Neither the Rights/Obligations Model nor the Fiduciary Model is an independently adequate safeguard for consumer privacy. Therefore, we propose drawing desirable features from each of the two to create a Hybrid Model. The Hybrid Model borrows from the rights and obligations in statutes that follow the Rights/Obligations Model but nests those obligations within broader information fiduciary duties. By combining strengths from the two models, businesses will still be on notice about what kinds of practices are expected of them but also must carefully consider how their data practices could harm consumers in other ways. We further propose incorporating the data controller/data processor distinction in the GDPR and existing U.S. state laws to (1) create a workable definition of "data fiduciaries" and (2) harmonize the language between U.S. state laws and the GDPR. We then take this proposal a step further by asserting that all businesses that fall within the scope of state consumer privacy laws should be considered "data controllers" by default and should bear the burden of proof to rebut that presumption if they are alleged to have violated their legal duties.

A. The Definition: Data Controllers as Data Fiduciaries

Even where scholars have proposed varying frameworks and definitions for fiduciary-inspired duties, none have yet offered workable statutory language that could enact such duties. We propose defining data fiduciaries as "data controllers" for two reasons. First, the term captures the foundational theory underlying the Fiduciary Model in a more workable statutory framework. Second, the use of the terms in existing U.S. privacy law and the GDPR can leverage the so-called "California Effect"[145] and "Brussels Effect" to enable better compliance and greater efficiency from regulated entities.

145. "[T]he California Effect occurs when one jurisdiction pushes other jurisdictions to improve their own laws." Chander et al., *supra* note 71, at 1743.

1. Data Controllers as an Analog to Data Fiduciaries

While scholars have proposed a variety of means by which to qualify entities that collect or process personal data as fiduciaries (namely, fiduciaries that must fulfill duties across different contexts), these theoretical constructs are too underdeveloped as statutory definitions. Take, for example, Balkin's premise that online service providers ("OSPs") must meet three conditions to be an information fiduciary.[146] It is not entirely clear how these criteria would work in practice. For example, what would it mean legally to "hold oneself out" as a privacy-respecting organization? Would this apply only to companies like Apple, which advertise that they are privacy-conscious companies?[147] Is their mere adoption of the tagline, "Privacy. That's Apple."[148] sufficient to give users a reason to believe Apple will not misuse or disclose their personal information? It is not clear courts would agree that is the case, given the leeway courts give to advertisers to embellish their claims with "puffery."[149] Perhaps one could instead look to company privacy policies to determine what promises OSPs made to their end users regarding how the company will collect and use their data. However, privacy policies are notoriously ineffective "privacy theater,"[150] and more often than not function to shield companies from liability for whatever they choose to do with users' data.[151] As such, the existing legal

146. His three conditions are as follows: (1) they hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them; (2) they give users a reason to believe they will not misuse or disclose their personal information; and (3) the users reasonably believe these companies will not disclose or misuse their data based on existing social norms or patterns of practice. Balkin, *Information Fiduciaries, supra* note 86, at 1223–24.

147. Kate O'Flaherty, *Apple Slams Facebook and Google With Bold New Privacy Ad*, FORBES (May 25, 2022), https://www.forbes.com/sites/kateoflahertyuk/2022/05/25/apple-slams-facebook-and-google-with-bold-new-privacy-ad [https://perma.cc/D9QR-K8UC]; *Privacy. That's Apple.*, APPLE, https://www.apple.com/privacy [https://perma.cc/Y9DR-2K7U].

148. O'Flaherty, *supra* note 147; *Privacy. That's Apple*, *supra* note 147.

149. *See, e.g.*, Jessani v. Monini N. Am., Inc., 744 F. App'x 18 (2d Cir. 2018).

150. "[P]rivacy theater . . . seeks to heighten a feeling of privacy protection without actually accomplishing anything substantive in this regard." Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 310 (2008).

151. *See generally, e.g.*, Kristen Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, 18 FIRST MONDAY 1 (2013); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & POL'Y INFO. SOC'Y 543 (2008);

framework provides weak guidance on how one would determine when there is (or is not) a fiduciary relationship between an OSP and a user.

That being said, Balkin's theoretical groundwork provides guidance as to what concerns the Fiduciary Model is meant to address, which could help inform privacy legislation seeking to impose fiduciary duties. First, Balkin highlights the potential for misuse of information when there are asymmetries in power and information between users and OSPs.[152] Ariel Dobkin built on Balkin's theory and listed specific actions that would violate an information fiduciary duty: "(1) using [customers'] data to manipulate them; (2) using [customers'] data to discriminate against them; (3) sharing [customers'] data with third parties without consent; or (4) violating their own privacy policies."[153] By Dobkin's formulation, fiduciary duties are violated based on how information is used or processed—or rather, based on the choices data controllers make regarding how to use or process data.

On the other hand, there are scholars who support the notion of ascribing duties automatically whenever there is an information relationship between an individual and an organization. Richards and Hartzog suggest a duty should attach to organizations when users disclose information.[154] Professor Lauren Scholz and Professor Lindsay Barrett have independently made similar recommendations that duties should be compulsory in consumer relationships.[155] However, these broad definitions do not sufficiently detail in what contexts disclosure or collection of personal data should give rise to fiduciary duties.

Imposing fiduciary duties upon "data controllers" as defined in the GDPR provides a workable alternative. In the GDPR, a "data controller" is an entity that (1) has access to a user's personal data—either directly or through an intermediary; (2) has a commercial interest in a user's personal data; and (3)

Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357 (2022) (describing challenges to the current information privacy regime and proposed reforms); JOSEPH TUROW, YPHTACH LELKES, NORA A. DRAPER & ARI EZRA WALDMAN, AMERICANS CAN'T CONSENT TO COMPANIES' USE OF THEIR DATA (2023).

152. *See supra* Section III.A.

153. Dobkin, *supra* note 99, at 7, 17.

154. *See* Hartzog & Richards, *Legislating*, *supra* note 103, at 378.

155. *See* Barrett, *supra* note 99, at 1092–94; Scholz, *supra* note 99, at 187–91.

exerts influence over the processing of personal information—including collection, transmission, storage, and analysis of such data.[156] While these three factors are not directly analogous to the factors that give rise to information fiduciaries, they address similar problems of power and information asymmetries that the Fiduciary Model targets.[157] Entities that have access to such information, have a commercial interest in personal information, and have the ability to make decisions about how to use that data are in prime positions to take advantage of the very conditions that should give rise to information fiduciary duties: asymmetries of power, information, and transparency.[158] Users rarely know how or when the OSPs they interact with are collecting or processing their data (notwithstanding privacy policies), which creates information asymmetries.[159] Further, the scope limitations on U.S. state laws ensure that such laws are only targeting large companies or those that make most of their profits off of personal data. The kinds of large companies subject to state laws—like Meta, Apple, and Amazon—are the same kinds of companies that prove most difficult for consumers to avoid engaging with in some capacity, which gives rise to the power asymmetries.[160] The combination of information and power asymmetries incentivize company (mis)use of data.[161] As such, imposing fiduciary duties upon "data controllers" as defined in the GDPR—and with limitations in scope deemed suitable by state legislatures—provides an alternate mechanism to address the same issues the Fiduciary Model targets, with a definition already present in existing consumer privacy laws.

This approach is already being considered internationally. In November 2022, India's Ministry of Electronics and Information Technology introduced a draft of the "Digital Personal Data Protection Bill, 2022,"[162] which would make any

156. *See supra* Section I.A.

157. *See* Balkin, *Algorithmic Society*, *supra* note 112, at 1160–61.

158. *Id.*

159. *See, e.g.*, TUROW ET AL., *supra* note 151; Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words*, WASH. POST (May 31, 2022), https://www-washingtonpost-com.libproxy.lib.unc.edu/technology/2022/05/31/abolish-privacy-policies [https://perma.cc/4K4N-U3WG].

160. *See supra* Section II.A.

161. *See* Balkin, *Algorithmic Society*, *supra* note 112, at 1160–61.

162. Digital Personal Data Protection Bill, 2022 (India), https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf [https://perma.cc/B6PG-8G4J].

person "who alone or in conjunction with other persons determines the purpose and means of processing of personal data" a "data fiduciary" subject to various duties and obligations.[163] It should be noted, however, that although India uses the "data fiduciary" label, the duties and obligations imposed by its law would be more similar to the Rights /Obligations Model than data fiduciary duties—further illustrating the confusion around the existing Fiduciary Model and the need for clarification.[164]

2. Harmonizing U.S. Consumer Privacy Law with the GDPR

While it is not yet clear whether U.S. states will follow the European Union's interpretation of "data controller," because several states have already adopted the same terms, state agencies and courts will soon need to define them. As such, using these terms in other models of privacy regulation will make it easier and more efficient to diverge from the model that ten states have followed thus far. In addition, using the same terms as the GDPR can help harmonize some aspects of U.S. consumer privacy law with the GDPR.

Using language from the GDPR leverages the Brussels Effect. The Brussels Effect describes a market mechanism by which "market actors conform their global products to European rules."[165] This occurs because large, multinational corporations are incentivized to standardize their operations globally by adhering to a single rule, rather than attempting to separate their operations out by jurisdiction.[166] The Brussels Effect differs from the California Effect because the Brussels Effect describes the actions of corporations rather than lawmakers.[167] However, the Brussels Effect can have an impact on lawmaking, as demonstrated by the origins of the Washington privacy bill that several states have since adopted.[168] Businesses have a strong interest in consistent regulations across jurisdictions; the alternative is the costly and risky endeavor of navigating

163. *Id.* § 2(5).
164. *Id.* § 9.
165. Chander et al., *supra* note 71, at 1744.
166. *Id.* at 1745.
167. *Id.*
168. *See supra* Section I.B.

through a "regulatory thicket" of laws across multiple jurisdictions.[169]

Scholars have speculated that California would emerge as a "super-regulator" in the consumer privacy realm, in which other jurisdictions would adopt the same rules as California.[170] While this California Effect[171] has not happened yet, the latest consumer privacy laws passed in other states have much in common with California's laws, and many other states follow nearly the same model—namely, the failed Washington Privacy Act.[172] It is possible that this could indicate a "Washington Effect" of sorts, in which more states will continue to use the model initially introduced in the Washington legislature.[173] At the very least, states will likely continue to use the same terminology distinguishing between data controllers and data processors. To the extent that the United States is engaged in a state-level regulatory approach, incorporating this same language into other privacy regulations will make new laws easier to implement and understand from state to state. The New York Senate's bill imposing fiduciary-esque duties on data controllers and processors shows that this approach is already being considered in state legislatures.[174]

Although there are still ambiguities in the European Union as to who is and is not a data controller, the fact that several U.S. states have already adopted the same terms means that these terms are already set up to be defined by state agencies and courts.[175] Further, by limiting the scope of data controllers subject to state laws through business threshold requirements, some of the regulatory burdens in the EU definition of data controllers become less of a problem.[176] For example, in the

169. *See, e.g.*, Anupam Chander & Paul Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49, 76 (2023).

170. Chander et al., *supra* note 71, at 1742–44.

171. *Id.*

172. S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019); *see also* Chander et al., *supra* note 71, at 1733, 1788.

173. S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019).

174. *See* New York Privacy Act, S.B. A3593 (Feb. 3, 2023).

175. We acknowledge the risk that states may interpret their own laws differently. This is the inherent risk of state-level regulation as opposed to federal regulation.

176. *See* Anupam Chander, Alice de Jonge, Moritz Hennemann, Jan Kramer, Mike Liu & Marcelo Thompson, *Prospects for Harmonization of Global Data Governance*, *in* GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS 49, 55 (2022), https://cerre.eu/wp-content/uploads/2022/11/GGDE_FulIReport.pdf [https://perma.cc/J8JS-8WYG] (describing regulatory burdens from the GDPR, including

European Union, a small business owner who embeds a Facebook "like" button on their website would likely be considered a "data controller" subject to the GDPR requirements.[177] Under current U.S. state laws, that same small business owner may be considered a "data controller," but this analysis would not take place unless they had enough revenue or reached a high enough threshold of customers to fall within the scope of those laws in the first place.[178] As such, limits on scope can address some of the ways in which the European Union's interpretations of data controller may be too broad while still easing regulatory burdens on business by harmonizing some of the language in U.S. state consumer privacy law with the GDPR.

B. The Details: Presumptions and Burdens of Proof

Simply defining data fiduciaries as "data controllers" does not end the analysis, however. Even with set terms and definitions, legal factfinding, by nature, "involves decision-making under uncertainty."[179] To this end, the legal system has adopted burdens of proof; "a set of decision rules to instruct judges and jurors how to decide cases in the face of uncertainty."[180] Common burdens of proof are the well-known standard by which prosecutors must prove accusations against a defendant in criminal cases "beyond a reasonable doubt," or by a "preponderance of evidence" or "clear and convincing evidence" in civil cases.[181] Thus, a key question in the construction and application of consumer privacy laws not yet addressed in the literature is who should carry the burden of proof to establish whether an entity is or is not a data controller.

Burdens of proof encompass two different functions in litigation.[182] First is the burden of production, which entails

the fact that compliance burdens are especially high for small and medium-sized businesses).

177. *See supra* Section I.A.

178. *See supra* Section I.B.

179. Ronald J. Allen & Alex Stein, *Evidence, Probability, and the Burden of Proof*, 55 ARIZ. L. REV. 557, 558 (2013).

180. *Id.*

181. *Id.*

182. *Id.*; ROBERT P. MOSTELLER, KENNETH S. BROUN, GEORGE E. DIX, EDWARD J. IMWIKELRIED, D.H. KAYE & ELEANOR SWIFT, MCCORMICKS' EVIDENCE § 336 (8th ed. 2020) [hereinafter MCCORMICKS' EVIDENCE]; *see also* 21B CHARLES ALAN

producing satisfactory evidence to a judge of a particular fact at issue.[183] The party that bears the burden of production also risks an adverse ruling, such as a finding of fact or directed verdict, if they fail to produce evidence on an issue.[184] In most cases, the burden of production is first cast upon the party who pleads the existence of a fact.[185] In the context of consumer privacy law, this would mean a state attorney general or a citizen who brings a civil action against a data controller would initially bear the burden of producing evidence sufficient for a judge to find that the defendant is a data controller.

Second is the burden of persuasion, or the burden of persuading the factfinder that the alleged fact is true.[186] The burden of persuasion only comes into play if the parties have met their burdens of production.[187] In cases where there is uncertainty as to the existence of a fact, the trier of fact is instructed on how to decide the issue if they are in doubt—for instance, by a "preponderance of evidence" standard or a "clear and convincing" standard.[188] The preponderance of evidence standard means that the factfinder must find that the contested fact is more likely than not to be true—essentially, there must be a greater than 50 percent chance the contested fact is true.[189] In contrast, under the "clear and convincing" standard, the contested fact must be "highly probable."[190]

Presumptions function alongside burdens of proof to shift the burden from one party to another.[191] For example, if the party with the burden of production of Fact A introduces proof

WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 5122 (2d ed. 2022); Schaffer *ex rel.* Schaffer v. Weast, 546 U.S. 49, 56–57 (2005).

183. *See* WRIGHT & MILLER, *supra* note 182, at § 5122; MCCORMICKS' EVIDENCE, *supra* note 182, at § 336.

184. MCCORMICKS' EVIDENCE, *supra* note 182, at § 336 (2020)*; see also* Ronald J. Allen, *Presumptions, Inferences and Burden of Proof in Federal Civil Actions—An Anatomy of Unnecessary Ambiguity and a Proposal for Reform*, 76 NW. U. L. REV. 892, 895 (1982).

185. MCCORMICKS' EVIDENCE, *supra* note 182, at § 336*; see also* Allen, *supra* note 184, at 895; Gross v. FBL Financial Services, Inc., 557 U.S. 167, 177 (2009) (explaining that the default rule, absent statutory text to the contrary, is that plaintiffs bear the burden of proving their claims).

186. MCCORMICKS' EVIDENCE, *supra* note 182, at § 336*; see also* Weast, 546 U.S. at 56–57.

187. MCCORMICKS' EVIDENCE, *supra* note 182, at § 336.

188. *See id.* at §§ 336, 339, 340; Allen & Stein, *supra* note 179, at 558.

189. *See* Neil B. Cohen, *Confidence in Probability: Burdens of Persuasion in a World of Imperfect Knowledge*, 60 N.Y.U. L. REV. 385, 394 (1985).

190. MCCORMICKS' EVIDENCE, *supra* note 182, at § 340.

191. *Id.* § 342.

of Fact B, a judge may determine that Fact A can be inferred from Fact B, and therefore there is a presumption that Fact A is true.[192] This presumption would then shift the burden of producing evidence to rebut Fact A to the opposing party.[193]

In applying consumer privacy laws using the data controller /data processor distinction, the default against regulated businesses could go two ways. The first option is to presume by default that a business being sued under such a law is a data processor and to assign to the enforcer—be it a state attorney general or a citizen bringing a private right of action—the burden of proving that the business is a data controller. The second option is to alter the default and presume that a business subject to a state's consumer privacy law is a data controller, and then assign the business the burden of proving it is a mere data processor. Alternatively, if there is no presumed default against regulated businesses, the plaintiff could have the burden to prove that the defendant is either a controller or processor. Whatever the case, the allocation of the default presumption—whether a business is considered a controller or processor—shifts the burdens of production and persuasion to one party or the other.[194]

This Section argues that—for policy and administrability reasons—entities subject to consumer privacy laws should be considered data controllers by default. Making regulated entities presumptively data controllers serves to allocate the burden of proof to defendants in such cases. In other words, the defendant must (1) bring forward evidence to rebut the claim it is a data controller (the burden of production) and (2) convince the factfinder it is not a data controller (the burden of persuasion).[195] There are three relevant considerations in determining which party to a lawsuit should bear the burden of proof: policy, probability, and possession of proof.[196] Taken together, these factors support the conclusion that businesses

192. *Id.*
193. *Id.*
194. *See* G. Michael Fenner, *Presumptions: 350 Years of Confusion and It Has Come to This*, 25 CREIGHTON L. REV. 383, 383 (1992).
195. *See* Amanda Reid, *Deciding Fair Use*, 2019 MICH. STATE L. REV. 601, 615 (describing how burdens of proof operate in the fair use context); MCCORMICKS' EVIDENCE, *supra* note 182, at §§ 336, 342.
196. WRIGHT & MILLER, *supra* note 182, at § 5122; Allen, *supra* note 184, at 898–99.

falling within the scope of state consumer privacy laws should be considered data controllers by default.

1. Policy Considerations Favor Data Controllers as the Default

The policy factor asks the question: what would best vindicate the policy of the substantive law being enforced?[197] In answering this question, courts often choose to either "put a finger on the scale" to assist the party that is seeking to vindicate the policy of the substantive law or "place hurdles in the paths" of the party seeking to advance a position disfavored by the substantive law.[198] In the context of data fiduciaries, the underlying policy seeks to protect users from the various harms that arise from the aggregation of their data by companies that have an asymmetrical power balance.[199] Essentially, data fiduciaries address the fact that companies may possess large amounts of data about their consumers, but consumers know very little about how companies are using their data.[200] It follows, then, that defining companies with large amounts of personal data as "controllers" by default furthers the policy interest in addressing issues of transparency and accountability between companies that use data and the data subjects.

2. Probability Considerations Favor Placing the Burden of Proof on Data Controllers

The probability factor assesses the question: what is the most likely state of affairs in the situations in which lawsuits will arise?[201] Generally, courts will place the burdens of proof on the party asserting the least probable set of facts.[202] In the data fiduciary context, this is a relatively simple analysis: given the broad definition of "data controller," in most cases where a data

197. WRIGHT & MILLER, *supra* note 182, at § 5122.

198. *Id.*; *see also* Fireman's Fund Ins. Co. v. Videfreeze Corp., 540 F.2d 1171, 1175–76 (3d Cir. 1976).

199. *See* discussion *supra* Section II.A.

200. *Id.*

201. WRIGHT & MILLER, *supra* note 182, at § 5122.

202. *Id.*; *see, e.g.*, 20801, Inc. v. Parker, 249 S.W.3d 392, 397 (Tex. 2008) ("The comparative likelihood that a certain situation may occur in a reasonable percentage of cases should be considered when determining" how to allocate burdens of proof.).

fiduciary law—or another consumer privacy law using the controller/processor distinction—is violated, more often than not the entity that violates the law will be found to be a controller. This is particularly likely given the trend in current state consumer privacy laws to limit their scope to only the largest businesses collecting and processing consumers' data.[203] Thus, if a state attorney general or a citizen exercising a private right of action can make a prima facie case that a company violated a consumer privacy law, the presumption should be that the company is a data controller and the burden should shift to the company to rebut that presumption.

3. Possession of Proof Considerations Show the Burden Would Sit the Lightest on Data Controllers

Finally, courts will ask: which party has the best access to the evidence needed to prove the facts of the case?[204] The general rule is that if one party has superior access to the evidence needed to prove a fact, that party must bear the burden of proof.[205] In other words, "the burden should be cast 'on whom it would sit the lightest.'"[206] Companies that process personal data bear the lightest burden to rebut the presumption that they are data controllers. The "processor" category is already a narrow one, and to qualify as a data processor, the company typically would have clear contractual guidelines set forth by a data controller.[207] As such, if a company is a processor rather than a controller, it should be relatively easy to produce proof of its relationship to a data controller—like contract terms or proof of monitoring and supervision by the controller—to such a degree that would categorize that company as a processor rather than a controller. On the other hand, it would be much more difficult for a state enforcer or private litigant to gather internal evidence from a company about its role in data processing.[208] As such, the

203. *See supra* Section I.B.

204. WRIGHT & MILLER, *supra* note 182, at § 5122.

205. *Id.*; *see also* United States v. Continental Ins. Co., 776 F.2d 962, 964 (11th Cir. 1985) ("[T]he party in the best position to present the requisite evidence should bear the burden of proof.").

206. WRIGHT & MILLER, *supra* note 182 (quoting Bentham in James B. Thayer, *The Burden of Proof*, 4 HARV. L. REV. 45, 59 (1890)).

207. *See supra* notes 58–64 and accompanying text.

208. The law has sometimes made it hard to state a claim pre-discovery. *See generally, e.g.*, A. Benjamin Spencer, *Pleading and Access to Civil Justice: A Response to Twiqbal Apologists*, 60 UCLA L. REV. 1710, 1710 (2013) (describing

burden of production sits the lightest on the companies processing data, particularly given the trend to limit the scope of state consumer privacy laws to only the largest businesses or those who make a significant portion of their revenue from processing data. These companies are more likely to be considered "controllers" rather than processors to begin with.

CONCLUSION

It is encouraging to see U.S. states' forward momentum in passing privacy laws. Nevertheless, the emerging model still needs improvement to ensure sufficient consumer privacy protection. The Rights/Obligations Model guarantees some rights to consumers but in doing so excludes other rights and leaves room for companies to negotiate carve-outs to their obligations. Another important problem is the trend away from creating private rights of action. Without a private right of action, those most vulnerable to misuse of their data will not always have an opportunity to vindicate their rights. Even with a private right of action, it is not clear that the Rights /Obligations Model defines harms in a way that would be sufficient to establish standing in court.

The Fiduciary Model supplements the Rights/Obligations Model by creating more flexible rights and duties that close regulatory gaps and future-proof the law. Merging these two models into a Hybrid Model has the potential to recognize harms to consumers that will be sufficient to establish Article III standing. We acknowledge that the Fiduciary Model is open to critique, notably for its vagueness and its failure to address the myriad antitrust issues that stem from the unchecked power of large platforms. Our response is twofold. First, the Fiduciary Model is not intended as a "silver bullet" that will fix every problem created by large platforms' aggregation of personal data. And second, the Fiduciary Model is an important tool in the "regulatory toolbox"[209] that, in combination with features of

notice pleading in federal courts as a "plausibility-pleading system that screens out potentially meritorious claims that fail to offer sufficient specificity and support at the pleading stage."); Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007); Ashcroft v. Iqbal, 556 U.S. 662 (2009). Changing presumptions not only puts the burden in the right place, it also safeguards against dismissal where a plaintiff may not be able to plausibly state a claim without access to a company's information.

209. *See* Grimmelmann, *supra* note 132.

the Rights/Obligations Model, can create a superior approach to addressing consumer privacy issues.

Blending the Fiduciary Model and the Rights/Obligations Model is the best way to futureproof the law, fill gaps in the existing legal framework, and address unremedied harms. Within our Hybrid Model, we provide much needed clarity. First, we recognize that the current trend in U.S. state laws is to distinguish between data controllers and processors. This categorization is already built in at the international level and continues to be adopted globally. As such, we propose to leverage this language to define data fiduciaries as "data controllers" to clarify who data fiduciary duties should apply to and to harmonize U.S. law with the GDPR. Further, by proposing a presumption that data holders subject to consumer privacy laws be considered "data controllers," we take into account important policy, probability, and possession considerations to suggest a workable framework for future privacy legislation.