# The Data Trust Solution to Data Sharing Problems

*Kimberly A. Houser*[*] *& John W. Bagby*[**]

**ABSTRACT**

*A small number of large companies hold most of the world's data. Once in the hands of these companies, data subjects have little control over the use and sharing of their data. Additionally, this data is not generally available to small and medium enterprises or organizations who seek to use it for social good. A number of solutions have been proposed to limit Big Tech "power," including antitrust actions and stricter privacy laws, but these measures are not likely to address both the oversharing and under-sharing of personal data. Although the data trust concept is being actively explored in the United Kingdom, European Union, and Canada, this is the first Article to take an in-depth look at the viability of data trusts from a US perspective. A data trust is a governance device that places an independent fiduciary intermediary between Big Tech and human data subjects. This Article explores how data trusts might be configured as bundles of contracts in the information supply chain. In addition to their benefits for the social good, data trusts might contribute to relieve some of the tension between EU and US privacy practices.*

[*] Clinical Assistant Professor, University of North Texas, and Visiting Scholar, Indiana University Bloomington, Ostrom Workshop. The authors wish to thank the members of the Data Trust Salon (Ostrom Workshop) for their presentations on the various forms and purposes for which data trusts may be created and the participants at the 2021 Law and Ethics of Big Data Colloquium co-hosted by the Pamplin School of Business at Virginia Tech (Janine Hiller) and the Kelley School of Business at Indiana University (Angie Raymond), and co-sponsored with the coordination of the planning committee of Deven Desai (Georgia Tech), David Nersessian (Babson), Kevin Werbach (Wharton), and Margaret Hu (Penn State) for their helpful remarks.

[**] Professor Emeritus, Colleges of Information Sciences & Technology and Smeal College of Business, the Pennsylvania State University.

**TABLE OF CONTENTS**

## I. INTRODUCTION

A small number of large companies (Big Tech) hold most of the world's data[1] and are able to determine with whom the data is shared or is not shared.[2] Most of these large data accumulators are located in the United States, where data protection laws are lacking.[3] For decades, regulators in the United States have taken a hands-off approach, permitting Big Tech to consolidate its power.[4] Data on its own is neither bad nor good; it is necessary for various subfields of artificial intelligence (AI) and highly valued by those who possess it.[5] However, private and concentrated power over the use and sharing of data has harmful consequences to the data subjects providing the data and to those denied access to the data.[6] Data security incentives, such as

---

1. *See* Bhaskar Chakravortl, *Big Tech's Stranglehold on Artificial Intelligence Must Be Regulated*, FOREIGN POL'Y (Aug. 11, 2021, 6:49 AM), https://foreignpolicy.com/2021/08/11/artificial-intelligence-big-tech-regulation-monopoly-antitrust-google-apple-amazon-facebook/?tpcc=re-circ_latest062921 [https://perma.cc/4SU9-9XDS]. **"**Data" has numerous meanings in various contexts. Herein, we largely use the term to refer to information collected electronically. *Compare* Robert I. Field, Ethan Dombroski, Mary Kate McDevitt & Whitney A. Petrie, *Genetic Databases and the Future of Medicine: Can Law and Ethics Keep Up? Perspectives and Analysis of a Conference*, 13 DREXEL L. REV. 321, 326 (2021) (explaining genetic data), *and* Teresa Scassa, *Public Transit Data Through an Intellectual Property Lens: Lessons About Open Data*, 41 FORDHAM URB. L.J. 1759, 1759 (2014) (explaining open data), *with* Timothy M. Snyder, Note, *You're Fired! A Case for Agency Moderation of Machine Data in the Employment Context*, 24 GEO. MASON L. REV. 243, 251 (2016) (explaining machine data is information obtained from a process called machine learning).

2. *See* Chakravortl, *supra* note 1 (naming Apple, Facebook, Microsoft, Amazon, and Alphabet (Google's parent company)).

3. *See* Dimitri Shelest, *Big Tech Isn't Breaking Any Privacy Rules if There Aren't Rules to Break*, CPO MAG. (Dec. 27, 2021), https://www.cpomagazine.com/data-privacy/big-tech-isnt-breaking-any-privacy-rules-if-there-arent-rules-to-break/ [https://perma.cc/BV9W-S9H7].

4. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters),* WIRE CUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/738D-TJ4W] ("The data collected by the vast majority of products people use every day isn't regulated. Since there are no federal privacy laws regulating many companies, they're pretty much free to do what they want with the data, unless a state has its own data privacy law. [However, a lot of the state laws are "business-model affirming."]"); *See also* Rebecca Crootof & B.J. Ard, *Structuring Techlaw*, 34 HARV. J.L. & TECH. 347, 358, 360, 367–68 (2021) (explaining the insufficiency of current regulations to address emerging technologies).

5. *See* Allison Grande, FTC's Brill Urges States To Prod Passive Data Brokers, Law360 Apr. 15, 2013, 7:48 PM), https://www.law360.com/articles/432886/ftc-s-brill-urges-states-to-prod-passive-data-brokers- [https://perma.cc/3ZF6-DMV3]; *see also* Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106, 122 (2019). *See generally* Rancho Labs, *6 Major Sub-Fields of Artificial Intelligence*, MEDIUM (Jul. 14, 2021), https://rancholabs.medium.com/6-major-sub-fields-of-artificial-intelligence-77f6a5b28109 [https://perma.cc/NN5W-KLKK].

6. *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. POL'Y FOR INFO. SOC'Y 425, 433, 456 (2011).

proprietary exploitation and accuracy, provide some relief.[7] But under US federal law, Big Tech has no reason to follow suit—its only duties demand that it use "reasonable measures" to prevent data breaches,[8] comply with its own terms of use and privacy policy,[9] and abstain from "unfair or deceptive acts or practices."[10]

This Article addresses the twin problems with the oversharing and under-sharing of consumer data. Not only are data subjects unable to identify and limit the use of their data in the United States,[11] but this data is also not generally available to smaller companies, nonprofits, or academia.[12] The hoarding of data by Big Tech also has the effect of inhibiting the use of AI[13] for social good.[14] While some have encouraged

---

7. *See generally* JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON US INDIVIDUALS 8 (2021), https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/J66Y-ZPYL].

8. *See, e.g.*, 16 C.F.R. § 682.3 (2022).

9. *See, e.g.*, *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement [https://perma.cc/CF6B-AZUH] (last visited Nov. 3, 2022) ("The FTC has been the chief federal agency on privacy policy and enforcement since the1970s, when it began enforcing one of the first federal privacy laws—the Fair Credit Reporting Act.").

10. FTC, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY (2021) (explaining "In lieu of a general privacy or security law, the [FTC's] primary source of legal authority in the privacy and data security space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial acts or practices."); *see also* Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC BUS. BLOG (Apr 19, 2021, 9:43 AM), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai [https://perma.cc/5244-N436]. Note that while there are specific statutory requirements regarding the use of financial, medical and children's data, most data collected by Big Tech does not fall within these categories. *See* Klosowski, *supra* note 4.

11. *See* Alessandro Acquisti, Curtis R. Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 442, 464 (2016).

12. *See Your Data Is Shared and Sold…What's Being Done About It?,* KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/38K3-845G] (explaining that big tech companies have a disincentive to share the data they collect because its possession creates a competitive advantage for that company) [hereinafter *Your Data Is Shared*]. We use the term data subjects throughout to describe those using the internet and connected devices from which Big Tech pulls their data.

13. AI is a data intensive, algorithmic-based computer assisted mimicking of human reasoning process that uses new data in machine learning; AI is generally divided into the categories of expert systems, robotics, autonomous systems, neural networks, and machine learning. *See generally* Ed Burns, *What Is Artificial Intelligence?*, TECHTARGET, https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence [https://perma.cc/V4U8-3XT3] (last visited Nov. 3, 2022, 5:58 PM).

14. *See* Bertin Martens, *The Importance of Data Access Regimes For Artificial Intelligence and Machine Learning* 5 (JRC Digital Economy Working Paper 2018-09, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3357652 [https://perma.cc/YP8M-74D5]; *see also* Viktor Mayer-Schönberger & Thomas Ramge, *Big Tech Is Hoarding the Data that Humanity*

antitrust actions against these large firms,[15] others have called for US laws patterned on the General Data Protection Regulation (GDPR).[16] As neither solution will address *both* the under- and oversharing of data, the data coffers of Big Tech will continue to grow, further concentrating their power.

Despite the "invisible hand" theory of markets, which proposes that they roughly channel society towards "optimal" outcomes,[17] considerable law-and-economics literature now demonstrates (i) a stubborn proliferation of market imperfections (e.g., imperfect competition, concentrated market power, asymmetric and imperfect information)[18] showing the insufficiency of the laissez-faire approach to achieve social goals,[19] and (ii) markets too often correct themselves at glacial speeds, resulting in regulatory lag that leaves the public vulnerable to many risks.[20]

The data trusts envisioned here adopt a longstanding approach that resolves this market failure. The Authors concede that markets can fail, yet the resolution of problems can still harness market forces.[21]

---

*Needs to Thrive*, TIME (June 8, 2022, 12:14 PM), https://time.com/6185433/big-tech-hoarding-data-humanity-needs/ [https://perma.cc/9LHQ-JDPL]; Prash Chandramohan, *The Importance of Data Sharing in Organizations*, MDM – A GEEK'S POINT OF VIEW (Oct. 26, 2020) https://www.mdmgeek.com/2020/10/26/the-importance-of-data-sharing-in-organizations/ [https://perma.cc/E6MK-UG82].

15. *See* Maurice E. Stucke, *Here Are All the Reasons It's a Bad idea to Let a Few Tech Companies Monopolize Our Data*, HARV. BUS. REV. (Mar. 27, 2018), https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data [https://perma.cc/K88X-TEGX].

16. *See* Joseph Duball, *EC Calls for Harmonization, Addresses Data Transfers in GDPR Review*, IAPP (Jun. 24, 2020), https://iapp.org/news/a/ec-calls-for-harmonization-increased-re-sources-in-gdpr-review/ [https://perma.cc/VRX8-PYE5] (European Commission Vice President for Values and Transparency Věra Jourová calls for harmonization of data protection regulations).

17. *See* Noah Rich, *Why the Invisible Hand?*, MICHIGAN J. ECON. (Jan. 14, 2022), https://sites.lsa.umich.edu/mje/2022/01/14/why-the-invisible-hand-an-analysis/ [https://perma.cc/YR4U-64RU].

18. *See* George A. Akerlof, *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 494 n.5 (1970).

19. On the denigration of reliance on transactions of the mythical "rational man" to govern society, see generally Robert A. Prentice & Jonathan J. Koehler, *A Normality Bias in Legal Decision Making*, 88 CORNELL L. REV. 583, 584–86 (2002) (recounting how law and economics scholars are in at least partial retreat as scientific evidence accumulates that decision making violates rigid rationality across many contexts). The literature on efficacy of antitrust and regulation as a cure to market failure (imperfections) is too voluminous to discuss here.

20. *See* John W. Bagby & Nizan Geslevich Packin, *RegTech and Predictive Lawmaking: Closing the RegLag Between Prospective Regulated Activity and Regulation*, 10 MICH. BUS. & ENTREPRENEURIAL L. REV. 127, 127, 151 (2021) (modeling regulatory lag to enable regulatory technologies (RegTech) that more promptly address societal damage).

21. *See* Aluma Zernik, *The (Unfulfilled) Fintech Potential*, 1 NOTRE DAME J. EMERGING TECH. 352, 355, 374–75 (2020).

The data trust approach simultaneously maintains some liberty while minimizing the predictable and more harmful negative externalities stubbornly plaguing many, if not most, markets.[22] This Article argues that the markets for personal data are riddled with imperfections, largely due to the market power of Big Tech and the public's poor understanding of its incentives and business practices.[23] Additionally, this Article argues that the industrial organization of Big Tech, information brokers, hoarders, and users should be restructured through the intervention of fiduciary-intermediaries operating data trusts as proposed here and elsewhere.[24] This market evolution could release a considerable amount of value currently locked up by oligopolistic domination. Further, this Article argues that drastic improvements in privacy protection are possible, enhancing security and incentivizing the future of analytics based on AI. Moreover, data trusts may reveal "black box" algorithms that leading technology firms use to concentrate their power and perpetuate injustices.[25] When information is released from monopolistic control, this transparency becomes the very sunlight that disinfects algorithmic wrongdoing and self-interest in industries reliant on Internet-dominated data collection, analysis, and use.[26]

Enabling data trusts will provide a voice for data subjects while incentivizing the sharing of data through appropriate data governance. These devices can serve as vehicles for the responsible sharing of data, which will not only rein in the hoarding of data by large tech companies, but also mitigate individual and collective harms from the oversharing

---

22. *See* Anouk Ruhaak, *How Data Trusts Can Protect Privacy*, MIT TECH. REV. (Feb. 24, 2021), https://www.technologyreview.com/2021/02/24/1017801/data-trust-cybersecurity-big-tech-privacy/ [https://perma.cc/4AZM-2JP5].

23. *See infra* Part II.

24. *See, e.g.,* Sylvie Delacroix & Neil D. Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance,* 9 INT'L. DATA PRIV. L. 236, 236, 252 (2019) (arguing for individual humans' data held for their benefit in a trust relationship operated by fiduciary trustees).

25. *See, e.g.,* Scott J. Shackelford, Isak Nti Asare, Rachel Dockery, Anjanette Raymond & Alexandra Sergueeva, *Should We Trust a Black Box to Safeguard Human Rights? a Comparative Analysis of AI Governance,* 26 UCLA J. INT'L L. & FOREIGN AFF. 35, 51, 68 (2021) (arguing AI algorithms make recommendations or directly implement decisions without clear audit trail of their decisionmaking impeding recourse by subject individuals).

26. *See* Nicol Turner Lee, Paul Resnick & Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms,* BROOKINGS INST. (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ [https://perma.cc/2VM5-3YS5]; *see also* REVA SCHWARTZ, APOSTOL VASSILEV, KRISTEN GREENE, LORI PERINE, ANDREW BURT & PATRICK HALL, TOWARDS A STANDARD FOR IDENTIFYING AND MANAGING BIAS IN ARTIFICIAL INTELLIGENCE 77 (2022).

of data.[27] Although data trusts have been richly explored in Canada,[28] the United Kingdom[29] and the European Union,[30] this Article examines the novel viability of data trusts from a US perspective.

Part II provides a brief overview of the types of individual and collective harms that stem from the inadequate regulation of data sharing and illustrates how data hoarding harms small and medium enterprises (SMEs) and prevents the advancement of AI for social good. Part III reviews potential data sharing models, including data cooperatives and data pools, contractual and corporate agreements, and data trusts. Part IV details how data trusts can serve as a viable solution to address problems in the current paradigm by providing stewardship over data through an independent fiduciary. After describing proposed data trust variants, this Article breaks down data trusts, theorizing them as a bundle of contracts and concluding with an explanation on how they can be deployed to automate the negotiation of data use. Part IV summarizes the Article's conclusions and suggests avenues for further exploration.

## II. DATA SHARING PROBLEMS

Data subjects are the individual humans whose data are hoarded by Big Tech.[31] These humans have personally identifiable information (PII) but are generally unable to identify who collects or archives their PII, so they are unable to police the use of their data in the United States.[32] Furthermore, this data is not generally available

27. *See* Delacroix & Lawrence, *supra* note 24, at 236.

28. *See Digital Content Governance and Data Trusts — Diversity of Content in the Digital Age*, DEP'T CAN. HERITAGE (Feb. 2020), https://www.canada.ca/en/canadian-heritage/services/diversity-content-digital-age/digital-content-governance-data-trust.html#a2 [https://perma.cc/YTP8-YWR8].

29. *See Data Trusts: Lessons from Three Pilots*, OPEN DATA INST. (Apr. 15, 2019), https://theodi.org/article/odi-data-trusts-report/ [https://perma.cc/3GK4-W3TA].

30. *See* European Commission, Directorate-General for Communications Networks, Content and Technology, *Commission Staff Working Document Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)* 73 (Nov. 25, 2020).

31. Although there are multiple definitions of data subjects, this Article refers to those from whom data is obtained through electronic means. *See, e.g.*, Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) (EU) [GDPR] (defining a data subject as "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"). This Article uses the terms more broadly.

32. *See* Acquisti et al., *supra* note 11, at 442, 464.

to smaller tech firms, nonprofits, or academia.[33] Because data is so valuable to machine learning, AI innovations, and the predictions based thereon, the hoarding of data by Big Tech prevents the use of AI for social good.[34] There is a plethora of scholarship detailing the potential and actual privacy harms that have arisen since the advent of the internet.[35] Here, we focus on the twin problems of over- and under-data sharing.[36] Unrestrained and irresponsible data sharing has long been a thorn in the European Union's side, resulting in stricter regulations[37] and a series of enforcement actions against US tech firms and others.[38] However, no jurisdiction has yet addressed the hoarding of data by Big Tech.[39] This failure to share data with academia, nonprofits, and SMEs has resulted in a self-serving feedback loop that increases the size and influence of Big Tech while preventing other actors from benefiting from these large data sets.[40] This Section briefly describes some of the harms

33. *See Your Data Is Shared, supra* note 12, at 796 n.1, 832, 833 n. 223, 841–42 (explaining that Big Tech companies have a disincentive to sell the data they collect because its possession creates a competitive advantage for that company).

34. *See supra* note 14.

35. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 796 n.1, 832, 833 n.223, 841–42 (describing physical, economic, reputational, discrimination, relationship, psychological, and autonomy harms from data privacy violations); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 673–74, 677 (2016); *see* ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 24, 64, 84 (2d ed. 2016) (describing how predictive analytics are currently being used by the government and business to identify preferences and risks and noting that the use of data about groups that have been historically discriminated against can result in discriminatory outcomes); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 85 (2015) (discussing potential risks of big data); Kate Crawford, *The Hidden Biases in Big Data*, HARV. BUS. REV. (Apr. 1, 2013), https://hbr.org/2013/04/the-hidden-biases-in-big-data [https://perma.cc/LQ69-BXBY].

36. *See Your Data Is Shared*, *supra* note 12. Oversharing generally refers to passing PII onward from a data collector to others without the subject individual's permission. By contrast, undersharing is the depriving of small entities and researchers from data that would inspire useful research or other services to the subject individual or other entities. *See id*.

37. See Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or A New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. no. 1, ¶¶ 2–4 (2018).

38. *See id*. at ¶¶ 20–35.

39. Thomas Tombal, *The Rationale for Compulsory B2B Data Sharing and Its Underlying Balancing Exercises*, 84 Revue du Droit des Technologies de l'information [R.D.T.I.] 5, 17 n.78 (2022) (Fr.) (listing all of the jurisdictions calling for mandatory data sharing legislation).

40. *See* Aaron Holmes, *Lawmakers say Facebook and Google Are Hoarding People's Personal Data and Using It to Grow in a 'Feedback Loop' Of Market Power—With No Intention to Stop*, INSIDER (Oct. 14, 2020, 10:24 AM), https://www.businessinsider.com/facebook-google-personal-data-privacy-congress-house-antitrust-report-2020-10. [https://perma.cc/TB9E-HYWL].

> For instance, 45% of Americans get their news on Facebook, which generally consumes an average of fifty minutes of its users' time every single day. Google, Microsoft, and Yahoo together control 98% of the [United States] search-engine market. Amazon

resulting from these twin problems: the over- and under-sharing of data by Big Tech.

### *A. Harms to Data Subjects*

While consumers clearly understand that they are sharing their data online with a website or platform, they are less certain of what exactly is being collected and what happens to that data afterwards.[41] When a data subject makes a post on Facebook, they understand that Facebook now has a copy of that post. However, when an Uber customer takes a ride in an Uber vehicle, Uber retains a record.[42] Most consumers fail to understand the full extent of the data these platforms gather, nor what happens to it afterwards.[43] Uber, for example, allowed company executives to predict "Rides of Glory" by analyzing trip data to forecast when users engaged in overnight liaisons.[44] Facebook tracks users' browsing information, *even when* users are not using Facebook, keeping a record of each search conducted online.[45] Google stores users' location data, which can be accessed by law enforcement through Google's *SensorVault* database indefinitely.[46] This location data is tracked and recorded *even when* the data subject is not using Google.[47] Federal law in the United States does not prohibit this collection and use, nor does it prohibit the sharing and selling of most types of data.[48] There is no

---

> accounts for 43% of [US] online retail sales. Facebook and Google control 73% of all digital advertising in the [United States].

Jennifer Shkabatur, *The Global Commons of Data*, 22 STAN. TECH. L. REV. 354, 393, 409 (2019).

41. *See* Andriy Slynchuk, *Big Brother Brands Report: Which Companies Might Access Our Personal Data the Most?,* CLARIO BLOG (Jul. 22, 2021), https://clario.co/blog/which-company-uses-most-data/ [https://perma.cc/2K39-L22B] (detailing the types of information collected by Big Tech and what can be done with it).

42. *See Uber Privacy Notice*, UBER, https://www.uber.com/legal/en/document/?country=united-states&lang=en&name=privacy-notice [https://perma.cc/9Z2G-QBES] (Oct. 13, 2022).

43. Acquisti et al., *supra* note 11, at 442, 464.

44. *See* Kurt Mueffelmann, *Uber's Privacy Woes Should Serve As a Cautionary Tale for All Companies*, WIRED, https://www.wired.com/insights/2015/01/uber-privacy-woes-cautionary-tale/ [https://perma.cc/8SRY-74SX] (last visited Nov. 3, 2022)**;** *see also*, John M. Jordan*, Challenges to Large-Scale Digital Organization: The Case of Uber*, 6 J. ORG. DESIGN no. 11, 2017, at 1, 3–4 (discussing privacy intrusion of Uber's God View feature).

45. *See* Nihal Krishan, *Four Hidden Ways Big Tech Platforms Suck Up Your Data*, COLO. POL. (Jun. 21, 2021), https://www.coloradopolitics.com/news/four-hidden-ways-big-tech-platforms-suck-up-your-data/article_1ada046c-e04f-51d8-bd57-2821bd65aab5.html [https://perma.cc/GL86-9L3S].

46. *See id*.

47. *See id.*

48. *See* Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—and How to Change the Game*, BROOKINGS INST. (Jul. 12, 2018), https://www.brookings.edu/research/why-

requirement to obtain consent from data subjects or inform them about with whom their data is shared or how it is used.[49] Indeed, a Pew research report indicates that, in the United States, 81 percent of people feel they have little to no control over corporate use of their personal data.[50] Even in the European Union, where websites are required to obtain the consent of data subjects to collect their data, most users just accept the use of cookies automatically to get access to the websites.[51]

It is not the individual data point (e.g., date of birth) that is collected by a company that holds the greatest potential for harm, but the ability of Big Tech and data brokers to combine and analyze the combination of collected data from other sources (e.g., zip code, SSN, street addresses, email, or IP address).[52] Such a combination, for example, could place the data subject at risk for identity theft, despite the data subject never providing their name to either website. As Sylvie Delacroix and Neil Lawrence, cofounders of the Data Trust Initiative hosted by the Universities of Cambridge and Birmingham, explain, data leaks on a daily basis[53]: "The systematic collection of data allows our lives to be dissected to an unprecedented degree. Although any individual fact learned about individuals may be inconsequential, when taken together, over time, a detailed picture emerges."[54]

---

protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/B95S-MXUZ] (explaining the insufficiency of US federal privacy law).

49. See Klosowski, *supra* note 4. The CCPA does give California residents the right to know what categories of information are being collected, the purpose of the collection, and the right opt out of the sale of their data. CAL. CIV. CODE §§ 1798.100, 1798.135.

50. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/GW5A-3SGT].

51. *See* Gry Hasselbalch & Pernille Tranberg, *Data Monopolies and Value Clashes*, DATA ETHICS (May 19, 2017), https://dataethics.eu/data-monopolies-value-clashes/ [https://perma.cc/TFD8-63RT]; *see also* Anouk Ruhaak, *When One Affects Many: The Case for Collective Consent*, MOZILLA FOUND. (Feb. 13, 2020), https://foundation.mozilla.org/en/blog/when-one-affects-many-case-collective-consent/ [https://perma.cc/AQQ4-FWRP] (explaining why notice and consent is an ineffective way to address data sharing and use).

52. *See* Cristian Santesteban & Shayne Longpre, *How Big Data Confers Market Power to Big Tech: Leveraging the Perspective of Data Science*, 65 ANTITRUST BULLETIN 459 (2020); *see also* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. REG. 667, 669, 671–72 (2017); Harry Guinness*, How Data Brokers Threaten Your Privacy*, POP. SCI. (May 25, 2022, 7:00 PM), https://www.popsci.com/technology/data-brokers-explained/ [https://perma.cc/UP6D-KNNY] (defining data brokers provisionally as entities that collect, improve, and sell PII to others by using data fusion of information collected, purchased or sensed from various sources using durable identifiers such as email address, phone numbers, street address, and SSNs).

53. Delacroix & Lawrence, *supra* note 24, at 237.

54. *Id.* at 237–238.

Our data can also be leaked by the actions of others.[55] This is especially true with genetic data, which can identify not just people who submit their data, but all those related to them.[56] Devices with which we have contact can also leak data.[57] These include our cars, "smart doorbells," outdoor cameras, digital assistants, wearable devices, thermostats, and license plate readers.[58] This constant leaking and collection of data presents privacy as well as civil rights concerns.[59] Harms noted include discrimination,[60] data breaches,[61] surveillance,[62] automated decision making,[63] and even data grabs by public authorities.[64]

---

55. *Id.* at 249.

56. *Id.* at 249.

57. *Id.* at 251; *see also* Ángel Díaz, *Law Enforcement Access to Smart Devices*, BRENNAN CTR. FOR JUST. (Dec. 21, 2020), https://www.brennancenter.org/our-work/research-reports/law-enforcement-access-smart-devices [https://perma.cc/Q558-Q758].

58. Díaz, *supra* note 57.

59. *See id.*; *see also* Deborah Hellman, *Big Data and Compounding Injustice*, J. MORAL PHIL. (forthcoming) (manuscript at 1) (explaining how flawed data can exacerbate data harms).

60. *See* Maria Bottis & George Bouchagiar, *Personal Data v. Big Data in the EU: Control Lost, Discrimination Found*, 8 OPEN J. PHIL. 192, 198 (2018) (describing how the mass collection of data can lead to discriminatory practices); Barocas & Selbst, *supra* note 35, at 674–75 (explaining how Big Data can reflect human biases leading to discrimination).

61. *See* Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion and the Modern Data Breach*, 69 FLA. L. REV. 771, 771 (2018) (describing the impact of data breaches).

62. Nicole McConlogue, *Discrimination on Wheels: How Big Data Uses License Plate Surveillance to Put the Brakes on Disadvantaged Drivers*, 18 STAN. J. C.R. & C.L. 279, 282, 342 (2022) (describing how Big Data harms stem from surveillance technologies).

63. Niklas Eder, *Beyond Automation: Machine Learning-Based Systems and Human Behavior in the Personalization Economy*, 25 STAN. TECH. L. REV. 1, 12 (2021) (explaining how algorithms are used to target ads and manipulate consumers).

64. Taylor Armerding, *The 5 Worst Big Data Privacy Risks (And How To Guard Against Them),* CSO (Jul. 14, 2017, 8:21 AM), https://www.csoonline.com/article/2855641/the-5-worst-big-data-privacy-risks-and-how-to-guard-against-them.html [https://perma.cc/LWY2-6SWK] ("According to EPIC, 'Americans are in more government databases than ever,' including that of the FBI, which collects personally identifiable information (PII) including name, any aliases, race, sex, date and place of birth, Social Security number, passport and driver's license numbers, address, telephone numbers, photographs, fingerprints, financial information like bank accounts, and employment and business information. Yet, 'incredibly, the agency has exempted itself from Privacy Act (of 1974) requirements that the FBI maintain only, 'accurate, relevant, timely and complete' personal records,' along with other safeguards of that information required by the Privacy Act, EPIC says. The NSA also opened a storage facility in Bluffdale, Utah, in 2014 that is reportedly capable of storing 12 zettabytes of data—a single zettabyte is the amount of information it would take 750 billion DVDs to store."); *see also* Nathan Freed Wessler, *The U.S. Government Is Secretly Using Cell Phone Location Data to Track Us. We're Suing*, ACLU (Dec. 2, 2020), https://www.aclu.org/news/immigrants-rights/the-u-s-government-is-secretly-using-cell-phone-location-data-to-track-us-were-suing/ [https://perma.cc/NU3J-XTZN] (describing how the federal government secretly purchases location data for the purpose of tracking people); Kimberly A. Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient*

All these data acquisition and processing methods permit additional data development.[65] For example, "derived data" is information that can be developed from multiple data points about an individual[66] or from an individual's relationship to a group.[67] Derived data is generally unknown to the individual and arises through the application of data analytics to a data set.[68] Because the data subjects do not provide this information directly, they are unaware that it has been inferred and collected.[69] This ability to not only infer new data, but to also make predictions based on it, presents serious, insidious issues because the individual cannot control the development of such information.[70] This is an especially risky concern with sensitive information like personal wealth and medical data.[71] Sensitive information can be sold and shared, presenting not only privacy harms but a financial windfall for the company that creates the new data.[72] While companies and the government increasingly use predictive analytics for efficiency,[73] failing to consider the source of the data used or its accuracy has resulted in significant harms to individuals,

*Solutions or the End of Privacy as We Know It?,* 19 VAND. J. ENT. & TECH. L. 817, 822, 847–48 (2017) (explaining how the government's use of data analytics violates privacy law); Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CTR. FOR JUST. (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data [https://perma.cc/UM4W-TU62] (describing how the government circumvents the Fourth Amendment with respect to the collection and use of citizen's personal information).

65. *See* Martens, *supra* note 14.

66. *See* Alda Yuan, *Derived Data: A Novel Privacy Concern in the Age of Advanced Biotechnology and Genome Sequencing*, YALE L. & POL'Y REV. INTER ALIA (Aug. 15, 2018, 12:15 PM), https://ylpr.yale.edu/inter_alia/derived-data-novel-privacy-concern-age-advanced-biotechnology-and-genome-sequencing [https://perma.cc/G5G5-SUPL].

67. *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 610 (2021) (calling for the democratic institution of data governance to address the wrongful amplification of social inequality).

68. *See* Yuan, *supra* note 66.

69. *See id.*

70. *See* Rainer Mühlhoff, *Predictive Privacy: Towards an Applied Ethics of Data Analytics*, 23 ETHICS & INFO. TECH. 675, 679–80 (2021), https://doi.org/10.1007/s10676-021-09606-x [https://perma.cc/Q46C-B39B] (explaining the harms resulting from predictive analytics using derived data); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 108, 111 n. 100 (2014); Rashida Richardson, Jason Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 192, 202 (2019), https://ssrn.com/abstract=3333423 [https://perma.cc/9P8Z-BP6L].

71. *See* Mühlhoff, *supra* note 70, at 682–85.

72. *See* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1012 (explaining that the sharing or leaking of sensitive data (e.g., health data) has the potential to generate the greatest harms (citations omitted)); *see also* SIEGEL, *supra* note 35, at 24.

73. Zarsky, *supra* note 72, at 1000.

including discrimination against women and certain racial groups.[74] Data mining[75] can be used to identify patterns and produce outcomes based on these data sets.[76] While many understand, or at least acknowledge, that product recommendations stem from the use of their online data and the data of others, few may understand how predictive analytics can limit their choices.[77] Additionally, the use of derived data can result in discriminatory outcomes in many industries, such as public safety, employment, advertising, and insurance underwriting.[78]

74. Barocas & Selbst, *supra* note 35, at 674 ("Approached without care, data mining can reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society. It can even have the perverse result of exacerbating existing inequalities by suggesting that historically disadvantaged groups actually deserve less favorable treatment."); Jessica K. Paulus & David M. Kent, *Predictably Unequal: Understanding and Addressing Concerns That Algorithmic Clinical Prediction May Increase Health Disparities*, 99 DIGIT. MED., no. 99, 2020, at 1, 4, https://www.nature.com/articles/s41746-020-0304-9 [https://perma.cc/QZZ7-WZFF] (explaining how bias in health data can lead to predictions resulting in punitive or coercive interventions and the misallocation of scarce resources).

75. Data mining is the data analysis step in the discovery of patterns extracted from large data sets using statistical and machine learning techniques. *See* Craig Stedman, *Data Mining*, TECHTARGET, https://www.techtarget.com/searchbusinessanalytics/definition/data-mining [https://perma.cc/H6HT-C8EQ] (last visited Nov. 3, 2022).

76. Rashida Richardson, *Addressing the Harmful Effects of Predictive Analytics Technologies*, GER. MARSHALL FUND (Nov. 19, 2020), https://www.gmfus.org/publications/addressing-harmful-effects-predictive-analytics-technologies [https://perma.cc/6CB6-47HZ].

77. Kimberly A. Houser, *Artificial Intelligence and the Struggle Between Good and Evil*, 60 WASHBURN L.J. 475, 480 (2021) [hereinafter Houser, *Artificial Intelligence*] ("As people rely more on AI-generated recommendations, they lose the ability to investigate and evaluate what they are purchasing. While many people consider it a "convenience" that products are brought to their attention based on their past purchasing history, it is also a serious loss of agency."); *see also, e.g., 'Recommended for You': How Well Does Personalized Marketing Work?*, KNOWLEDGE AT WHARTON (Dec. 4, 2015), https://knowledge.wharton.upenn.edu/article/recommended-for-you-how-well-does-personalized-marketing-work/ [https://perma.cc/R9W4-RNMV].

78. *See, e.g.*, Richardson et al., *supra* note 70, at 220 (discriminatory data results in discriminatory policing when predictive analytics are used); Paulus & Kent, *supra* note 74, at 1 (explaining that "predictive algorithms can inadvertently introduce unfairness in decision-making. This is a major concern as algorithmic technologies have permeated many important sectors: criminal justice (e.g., predicting recidivism for parole decisions); the financial industry (e.g., credit worthiness); homeland security (e.g., "no fly" lists); and targeted ads (e.g., job listings). Indeed, legislation has recently been proposed in the [United States] that would direct the Federal Trade Commission to require the assessment of algorithmic fairness and bias by entities that use, store, or share personal information for algorithmically supported decision-making.").

One especially nefarious use of derived data is by the police[79] and the judicial system.[80] For example, police forces have used predictive analytics to gauge likely future locations where crimes may occur.[81] These predeterminations often artificially concentrate a police presence in disproportionately low-income areas.[82] Moreover, judges and prosecutors have used data sets to set bail and calculate recidivism rates, but this usually results in discriminatory treatment between Black and White offenders.[83] The use of facial recognition to identify alleged criminals[84] has been demonstrated to work poorly on darker-toned faces, especially those of darker-toned women.[85] Using and combining data from multiple sources, each of which may contain inaccurate data,[86] exacerbates harm, particularly in the United States where no clear remedy yet exists.[87] When predictive analytics make decisions without explanation, a serious threat to human rights occurs.[88] Scholars Rashida Richardson, Jason Schultz, and Kate Crawford note that

> Law enforcement agencies are increasingly using predictive policing systems to forecast criminal activity and allocate police resources. Yet in numerous

79. Ángel Díaz, *Data-Driven Policing's Threat To Our Constitutional Rights*, BROOKINGS INST. (Sept. 13, 2021), https://www.brookings.edu/techstream/data-driven-policings-threat-to-our-constitutional-rights/ [https://perma.cc/5RTG-EVM5].

80. Judge Noel L. Hillman, *The Use of Artificial Intelligence in Gauging the Risk of Recidivism*, A.B.A. (Jan. 1, 2019), https://www.americanbar.org/groups/judicial/publications/judges_journal/2019/winter/the-use-artificial-intelligence-gauging-risk-recidivism/ [https://perma.cc/K395-T5HU].

81. Díaz, *supra* note 79.

82. Richardson et al., *supra* note 70, at 220.

83. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks,* PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/KAG8-NNBR]; *see also* Alexandra Chouldechova, *Fair Prediction With Disparate Impact: A Study Of Bias in Recidivism Prediction Instruments*, 5 BIG DATA 153 (2017).

84. Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1153 (2021); *see also* Tom Maxwell, *A Man Spent 10 Days in Jail Based on a Facial Recognition Error*, INPUT (Dec. 29, 2020), https://www.inputmag.com/tech/a-man-spent-10-days-in-jail-based-on-misclass ification-by-clearview-ai [https://perma.cc/BGC7-ZG35].

85. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 12 (2018).

86. *See generally* Jaap Wieringa, P. K. Kannan, Xiao Ma, Thomas Reutterer, Hans Risselada & Bernd Skiera, *Data Analytics in a Privacy-Concerned World*, 122 J. BUS. RSCH. 915, 917 (2021).

87. Molly K. Land & Jay D. Aronson, *Human Rights and Technology: New Challenges for Justice and Accountability*, 16 ANN. REV. L. & SOC. SCI. 223, 227 (2020); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1257–58, 1295 (2008) ("Automated systems impose accountability deficits that administrative procedures cannot remedy.").

88. Crawford & Schultz, *supra* note 70, at 106.

> jurisdictions, these systems are built on data produced during documented periods of flawed, racially biased, and sometimes unlawful practices and policies ("dirty policing"). These policing practices and policies shape the environment and the methodology by which data is created, which raises the risk of creating inaccurate, skewed, or systemically biased data ("dirty data"). If predictive policing systems are informed by such data, they cannot escape the legacies of the unlawful or biased policing practices that they are built on.[89]

Although some suggest that privacy law can be extended or strengthened to protect data subjects,[90] others point to studies demonstrating that neither the GDPR nor the California Consumer Privacy Act (CCPA), the two strongest privacy laws,[91] has resulted in "meaningful legal compliance" by Big Tech.[92] Such regulations rely on consumer complaints to the agencies for compliance, rather than active auditing.[93] In addition, despite the robust privacy protection scheme in the European Union's GDPR, data regulators seldom enforce these laws due to a lack of investigatory resources.[94] Some conjecture that the GDPR actually increases Big Tech's power.[95]

---

89. Richardson et al., *supra* note 70, at 192.

90. *See, e.g.*, Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation Is Just a Start*, BROOKINGS INST. (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ [https://perma.cc/9ZLZ-HU2F].

91. *See* Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 ME. L. REV. (forthcoming 2022) (manuscript at 17, 22). *Compare* CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2021) (providing data subjects with some rights *vis-à-vis* companies that collect data similar to the GDPR), *with* Council Regulation 2016/679, art. 1, 2016 O.J. (L 119) 32 (EU) [GDPR].

92. Lancieri, *supra* note 91, at 17.

93. *See, e.g.*, *What Should I Do If I Think That My Personal Data Protection Rights Haven't Been Respected?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/redress/what-should-i-do-if-i-think-my-personal-data-protection-rights-havent-been-respected_en [https://perma.cc/9UWL-FR7L] (last visited Nov. 6, 2022); *Frequently Asked Questions (FAQs)*, CAL., https://cppa.ca.gov/faq.html [https://perma.cc/TSK4-R9BC] (last visited Nov. 6, 2022).

94. Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 13, 2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement [https://perma.cc/ARK3-N9EG].

95. Christian Peukert, Stefan Bechtold, Michail Batikas & Tobias Kretschmer, *European Privacy Law and Global Markets for Data* (Ctr. for Econ. Pol'y. Rsch., Working Paper No. 01/2020, 2020) (documenting a reduction in market share by most firms after the introduction of the GDPR and an increase in market concentration in Big Tech after following more than 110,000 websites for eighteen months); Garrett Johnson, Scott K. Shriver & Samuel G. Goldberg, *Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR*, Paper presented at the American Economic Association and Allied Social Science Associations (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686 [https://perma.cc/B4FJ-RP2M] (finding that personal data collection became more concentrated after the GDPR, naming Google and Facebook as exemplars).

### *B. Obstacles to Cross-Border Data Sharing*

Data is held in locations around the world, and data flows are a constant reality.[96] Cross-border data transfers have increased exponentially over the past ten years (three trillion gigabytes of data moved around the world in 2020), and internet traffic is expected to increase another 50 percent from the 2020 level by the end of 2022.[97] A significant portion of this data is personal data.[98] Inconsistencies among the data-sharing regimes of foreign countries frustrate the efficient exchange of personal data.[99] For example, the European Union's strong privacy protections have frustrated cross-border data transfers from the European Union to the United States.[100] In 2020, the European Court of Justice (Schrems II) invalidated Privacy Shield,[101] which had previously permitted such cross-border transfers.[102] This decision risks the "$7.1 trillion transatlantic economic relationship" that has fostered trade and innovation between the United States and European Union.[103] Although in March 2022 the United States and European Union announced that they have agreed "in principle" to a new

96. *See infra* notes 383–85.

97. *Crossing Borders*, WORLD BANK, https://wdr2021.worldbank.org/stories/crossing-borders/ [https://perma.cc/YX7K-SLRE] (last visited Nov. 4, 2022).

98. *Id.*

99. *See id.* (map regarding open, conditional, and limited transfer rules).

100. The European Union requires "adequate assurances" that data transferred from the European Union to US companies will be protected. *See generally* Houser & Voss, *supra* note 37, at ¶ 101 (explaining the GDPR and its potential impact on US companies).

101. *See* Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd.*, ECLI:EU:C:2020:559 [Schrems II]. On July 16, 2020, the Court of Justice of the European Union issued a judgment declaring as "invalid" the European Commission's Decision (EU) 2016/1250 of July 12, 2016 on the adequacy of the protection provided by the EU-US Privacy Shield, finding that data protection laws in the US were insufficient. *See National Security Law—Surveillance—Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield.—Case C-311/18*, *Data Prot. Comm'r v. Facebook Ireland Ltd.*, *ECLI:EU:2020:559 (July 16, 2020)*, 134 HARV. L. REV. 1567, 1571 (2021) (explaining the decision and its limitations). The Privacy Shield permitted US companies to certify that they were meeting certain requirements of the GDPR. *See id.*

102. *See* Case C-362/14, *Schrems v. Data Prot. Comm'r*, ECLI:EU:C:2015:650, ¶¶ 6–28 [Schrems I].

103. *See* Press Release, Wilbur Ross, Secretary, Department of Commerce, Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://useu.usmission.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/ [https://perma.cc/SBW7-YTS3]. Because US companies collect data from both people and devices in the United States and European Union, this Article provides some analysis based on EU law to demonstrate its insufficiency in order to derail calls in the United States for a GDPR-type federal regulation or the breaking up of Big Tech. While the Authors do support omnibus privacy and data security law, it must be tailored to address data use. As explained *infra* Part V, placing the burden on data subjects will not reign in Big Tech, nor will "breaking up" Big Tech prevent harms.

Transatlantic Data Privacy Framework to permit data transfers from the European Union to the United States,[104] success will depend on US companies complying with the to-be-agreed-upon requirements.[105] The European Union is the United States' largest trading and investment partner,[106] and this failure to comply with the GDPR has long been a point of contention with EU data regulators.[107]

The contrast between these two regimes stems from ideological differences.[108] There is a strong economic incentive for the United States' free-market model, which mostly condones more aggressive and fugacious uses of data than under EU law.[109] The US tech industry accounts for 10.5 percent of the US GDP and 35 percent of the total world tech market.[110] On the other side of the Atlantic, the European Union adopts a rights-based approach, which relies on a regulatory vision that maximizes data subjects' individual control over their personal data.[111] This rights-based ideology underlies the European Union's GDPR.[112] However, the ever-increasing complexity of information systems using personal data challenges the European approach's success despite the steady progression of stronger data rights embodied in protective regulations.[113] Many feel that the European Union's approach has incapacitated its tech industry due to the industry's inability to employ data for use in developing AI

---

104. European Commission Press Release IP/22/2087, European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework (Mar. 25, 2022).

105. *See Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, WHITE HOUSE (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ [https://perma.cc/N5BB-JP7Y].

106. Houser & Voss, *supra* note 37, at ¶ 12.

107. *See id.* at ¶ 117; *see also* KRISTIN ARCHICK & RACHEL F. FEFER, CONG. RSCH. SERV., R46917, U.S.-EU PRIVACY SHIELD AND TRANSATLANTIC DATA FLOWS 1 (2021).

108. *See* Houser & Voss, *supra* note 37, at ¶¶ 18–19.

109. *See id.*

110. Jack Flynn, *25 Trending Tech Industry Statistics [2022]: The State of the U.S. Tech Industry*, ZIPPIA (Sept. 22, 2022), https://www.zippia.com/advice/tech-industry-statistics/ [https://perma.cc/LGW3-JU9R].

111. *See* ARCHICK & FEFER, *supra* note 107, at 5.

112. Council Regulation 2016/679, 2016 O.J. (L 119) (EU) [GDPR]. The EU parliament issues de jure regulations like the GDPR that are immediately enforceable in all member states (nations) but can also issue "directives" that are not immediately enforceable until implemented in each separate member state by national legislation. *See generally Sources and Scope of European Union Law*, EUR. PARL., https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law [https://perma.cc/EK9T-D5QV] (last visited Nov. 4, 2022).

113. *See* Daniel Castro & Eline Chivot, *Want Europe to Have the Best AI? Reform the GDPR*, IAPP (May 23, 2019), https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/ [https://perma.cc/9PN4-D93E].

systems.[114] According to Professor Lilian Edwards, "Big data is completely opposed to the basis of data protection. I think people have been very glib about saying we can make the two reconcilable, because it's very difficult."[115]

In addition to the differences in ideology between the United States and European Union around data protection, the two regimes also differ in their treatment and support of data sharing.[116] The following Section describes how SMEs are harmed by their lack of access to the data held by Big Tech.

### *C. Lost Opportunities from the Lack of Data Access*

SMEs are important for job growth, innovation, and the economy.[117] However, for a variety of reasons, these businesses are at an enormous disadvantage with respect to data analytics.[118] Big Tech has an incentive to limit access to the data it amasses.[119] First, by selling access to advertisers rather than selling the data itself, Big Tech can monetize the same data through multiple rounds of reselling.[120]

---

114. *See, e.g.*, Mirko Forti, *The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR*, 13 EUR. J. LEGAL STUD. 29, 31, 33 (2021); Zarsky, *supra* note 72, at 1004, 1008. For a detailed explanation of the proposed EU AI guidelines, see Wolfgang A. Maschek, Rosa Barcelo, Matthew Kirk, Georg Serentschy & Christina Economides, *The Proposed New EU Regulatory Regime for Artificial Intelligence (AI),* NAT. L. REV. (Sept. 17, 2021), https://www.natlawreview.com/article/proposed-new-eu-regulatory-regime-artificial-intelligence-ai [https://perma.cc/V5VB-QC6N].

115. Keith D. Foote, *Artificial Intelligence, Machine Learning, and Data Protection*, DATA DIVERSITY (Oct. 21, 2021), https://www.dataversity.net/artificial-intelligence-machine-learning-and-data-protection/ [https://perma.cc/66TD-GPPK] (explaining that the GDPR's purpose limitation, data minimization, transparency, and consent requirements are incompatible with machine leaning systems); *c.f.* Sci. Foresight Unit (STOA), Eur. Parliamentary Rsch. Serv., *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, at 76, PE 641.530 (Jun. 2020) (asserting that although AI is not incompatible with the GDPR, additional guidance is needed).

116. *See generally* Eur. Parliamentary Pol'y Dep't for Citizens' Rts. & Const. Affs., *A Comparison Between US and EU Data Protection Legislation for Law Enforcement*, PE 536.459 (Sept. 2015).

117. STEFAAN VERHULST & ROBYN CAPLAN, OPEN DATA: A TWENTY-FIRST CENTURY ASSET FOR SMALL AND MEDIUM-SIZED ENTERPRISES 10 (2015), https://thegovlab.org/static/files/publications/OpenData-and-SME-Final-Aug2015.pdf [https://perma.cc/MS82-PWQJ] (SMEs "are estimated to account for over 60 percent of new jobs created in the United States, and 60–70 percent of new jobs created across all OECD countries." (citations omitted)).

118. *Id.*

119. *See* Shkabatur, *supra* note 40, at 393, 409.

120. *See* Alfred Ng, *What Does It Actually Mean When A Company Says "We Do Not Sell Your Data"?*, MARKUP (Sept. 2, 2021, 8:00 PM), https://themarkup.org/the-break-down/2021/09/02/what-does-it-actually-mean-when-a-company-says-we-do-not-sell-your-data [https://perma.cc/W3KN-8KRE].

Second, Big Tech is able to expand its customer base due to its ease of use and recommendation services, and it can also keep the competition from gaining a foothold.[121] The US House of Representatives' Antitrust, Commercial, and Administrative Law Subcommittee recently issued a report demonstrating that this mass data collection creates monopolies where the SMEs cannot compete.[122] The reasons for the lack of competition are that Big Tech can use data to target consumers more efficiently and that customers are hesitant to switch to other providers due to the high cost and hassle.[123] These are switching costs, long recognized in law and economics as barriers to entry for new entrant competitors of any size.[124]

The pandemic has only amplified Big Tech's control over consumer data with the public's increased reliance on these companies to work, communicate, and learn.[125] As stay-at-home orders and uncertainty over the length and impact of the pandemic intensified, people increasingly conducted their lives and businesses online.[126] This shift during the pandemic "has led to outsized profits for these companies and concentrated even more power in their hands."[127]

---

121. *See* Shkabatur, *supra* note 40, at 357–58.

122. *See* STAFF OF S. SUBCOMM. ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW OF THE COMM. ON THE JUDICIARY, 116TH CONG., REP. ON COMPETITION IN DIGITAL MARKETS (2020); *see also* Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 43–44 (2019), (detailing why Big Tech's ability to utilize derived data constitutes anticompetitive conduct); Dina Srinivasan, *Why Google Dominates Advertising Markets*, 24 STAN. TECH. L. REV. 55, 59 (2020) (comparing Big Tech's "advertising exchanges" to the prohibited conduct of traded financial markets).

123. *See* Jane Thompson, *Big Tech, Big Data and the New World of Digital Health*, 5 GLOB. HEALTH J. 165, 166 (2021).

124. *See generally* Carl Shapiro & Hal R. Varian, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1998). *But see* Hal R. Varian, *Seven Deadly Sins of Tech?*, 54 INFO. ECON. & POL'Y (forthcoming).

125. *See* David Streitfeld, *How Tech Won the Pandemic and Now May Never Lose*, N.Y. TIMES (Oct. 12, 2021), https://www.nytimes.com/2021/07/23/technology/silicon-valleys-pandemic-profits.html?campaign_id=158&emc=edit_ot_20210729&instance_id=36566&nl=on-tech-with-shiraovide&regi_id=63754704&segment_id=64781&te=1&user_id=106bf8905aec42c3fa04c54a2525c8f6 [https://perma.cc/L4MK-HKG3] (noting, however, that this shift has brought increased attention to Big Tech by the government).

126. *See, e.g.*, *id.*

127. Chakravortl, *supra* note 1; *see also* Streitfeld, *supra* note 125 (During the pandemic, "[t]he combined stock market valuation of Apple, Alphabet, Nvidia, Tesla, Microsoft, Amazon and Facebook increased by about 70 percent to more than $10 trillion.").

Much of Big Tech's power comes from its platform business model.[128] The platform model enables Big Tech to serve as a connector through which nearly all data flows, observed by the platform operator.[129] The ability of the platform model to operate globally leads to oversized network effects.[130] In addition, Big Tech's large stores of consumer data provide it with an "unassailable competitive advantage."[131] According to MIT financial economist Andrew W. Lo, "for most companies, their data is their single biggest asset."[132]

The ability to control this data provides Big Tech with incredible market power.[133] In the European Union, antitrust actions also fail due to the focus on "economic orthodoxy."[134] The European Union's proposed Digital Markets Act (DMA) is considered[135] an evolution in antitrust law and a way to prevent Big Tech from engaging in unfair and anticompetitive businesses practices.[136] The DMA essentially focuses on the way in which Big Tech companies have become "gatekeepers" of

---

128. Pete Swabey & Martín Harracá, *Digital Power: How Big Tech Draws its Influence*, TECH MONITOR (July 29, 2022, 11:09AM), https://techmonitor.ai/policy/big-tech/power-of-tech-companies [https://perma.cc/L5GX-BN2H].

129. *Id.*

130. *Id.*

131. *Id.*

132. MIT TECH. REV. CUSTOM, THE RISE OF DATA CAPITAL 1 4, http://files.technologyreview.com/whitepapers/MIT_Oracle+Report-The_Rise_of_Data_Capital.pdf [https://perma.cc/V64R-DDSX] (explaining that data is a capital asset and serves as the raw material for new digital services).

133. *See* Santesteban & Longpre, *supra* note 52.

134. *See* Cristina Caffarra, Gregory Crawford & Johnny Ryan, *The Antitrust Orthodoxy is Blind to Real Data Harms*, VOX EU (Apr. 22, 2021), https://cepr.org/voxeu/blogs-and-reviews/antitrust-orthodoxy-blind-real-data-harms [https://perma.cc/TTL6-MFYC] ("Europe has had a data protection regulation (GDPR) since 2018, but with the exception of Germany and its Facebook case this has not spurred the European competition agencies (notably the EC) to pursue actual cases around data misuse as direct market power manipulation and extraction. In the main, the antitrust orthodoxy has continued to rely on its traditional tools."); Gadjo Sevilla, *Ireland's Failure to Enforce EU Law Against Big Tech Is Slowing Down Europe's GDPR Enforcement*, INSIDER INTEL. (Sept. 15, 2021), https://www.emarketer.com/content/ireland-s-failure-enforce-eu-law-against-big-tech-slowing-down-europe-s-gdpr-enforcement [https://perma.cc/897F-Z4Z8] ("The regulator [in Ireland] has left still unresolved 98% of 164 complaints against significant privacy abuses.").

135. For an excellent summary of the Digital Markets Act, see NATALIA MORENO BELLOSO, PROPOSAL FOR A DIGITAL MARKETS ACT (DMA): A SUMMARY (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3999966 [https://perma.cc/7CMS-CXW2].

136. *See* Aline Blankertz, *The EU's Experimental Approach in Overhauling Competition Rules*, BROOKINGS INST. (Apr. 14, 2022), https://www.brookings.edu/techstream/the-eus-experimental-approach-in-overhauling-competition-rules-digital-markets-act-dma/ [https://perma.cc/7ZVA-33DF].

data due to their massive data stores.[137] However, others doubt it will have the effect intended.[138]

Perhaps recognizing that the limitations on the use of data in the European Union have stymied their tech industry,[139] European lawmakers have proposed a new data strategy involving

> 'voluntary' data-sharing, in compliance with the GDPR, including 'data altruism,' where individuals can grant permission for their information to be used 'for the public good.' It would also include mandates supporting 'business-to-business data-sharing,' especially in industrial settings, and tackle APIs and other interoperability issues that businesses use to keep data proprietary.[140]

Referring to the "market imbalance" caused by Big Tech's hoarding of data, the European Union hopes to establish legislation that will encourage Big Tech to share its stores of data.[141]

In the United States, the 117th Congress proposed the ACCESS Act,[142] which would require Big Tech to make its data portable and interoperable, thus allowing consumers to move more easily from one service to another.[143] Requiring the sharing of data by Big Tech would

---

137. *See* Colin Wall & Eugenia Lostri, *The European Union's Digital Markets Act: A Primer*, CTR. FOR STRATEGIC & INT'L STUD. (Feb. 8, 2022), https://www.csis.org/analysis/european-unions-digital-markets-act-primer [https://perma.cc/MA86-ZGRS].

138. *See* Maurits Dolmans, Henry Mostyn & Emmi Kuivalainen, *Rigid Justice is Injustice: The EU's Digital Markets Act Should Include an Express Proportionality Safeguard*, ONDERNEMINGSRECHT, no. 1, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3985562 [https://perma.cc/XYT5-6FUQ] (providing a critique of the DMA).

139. *See, e.g.*, Castro & Chivot, *supra* note 113 ("The EU General Data Protection Regulation, which came into force a year ago, will affect the use of AI in at least three ways: by limiting the collection and use of data, restricting automated decision-making, and increasing compliance costs and risks. Unless the EU reforms the GDPR, Europe will fall behind others, such as the United States and China, in the development and use of AI."); Benjamin Mueller, *Europe's GDPR Regulators' AI Proposals Reveal Their Privacy Fundamentalism*, CTR. FOR DATA INNOVATION (July 29, 2021), https://datainnovation.org/2021/07/europes-gdpr-regulators-ai-proposals-reveal-their-privacy-fundamentalism/ [https://perma.cc/3B4G-V9MY] (explaining how EU regulations stifle the development of AI technologies in the European Union).

140. Kate Cox, *EU's New Digital Strategy Targets Data-Hoarding Tech Firms*, ARS TECHNICA (Feb. 20, 2020 12:51 PM), https://arstechnica.com/tech-policy/2020/02/facebook-google-would-have-to-share-more-data-under-new-eu-plan/ [https://perma.cc/3R49-ZKLL].

141. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM (2020) 66 final (Feb. 19, 2020) (calling for the sharing of data with SMEs).

142. Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021, H.R. 3849, 117th Cong. (2021).

143. Katharine Trendacosta, Bennett Cyphers, Cory Doctorow & Cindy Cohn, *The ACCESS ACT Takes A Step Towards A More Interoperable Future*, ELEC. FRONTIER FOUND. (Jun. 11, 2021), https://www.eff.org/deeplinks/2021/06/access-act-takes-step-towards-more-interoperable-future [https://perma.cc/2CA4-U3GL].

most certainly benefit small businesses—at least in theory.[144] Although a significant number of bills directed at Big Tech have been introduced in the United States, many (if not all) will never be enacted.[145] The next Section explains how more robust data sharing could result from more competition among enterprises seeking to use the data for social good.

### *D. Lack of Sharing for Social Good*

Although AI can be harnessed to solve social problems,[146] it needs data to work.[147] Machine Learning operates through new information inputs, such that robust AI requires data to achieve adaptation in dynamic environments.[148] Data sharing can create new opportunities to create social good.[149] Arguably, social good results from

144. For a description of the bill and its shortcomings, see *id.* and Bennett Cyphers & Cory Doctorow, *The New ACCESS Act Is a Good Start. Here's How to Make Sure It Delivers*, ELEC. FRONTIER FOUND. (Jun. 21, 2021), https://www.eff.org/deeplinks/2021/06/new-access-act-good-start-heres-how-make-sure-it-delivers [https://perma.cc/H654-WJP4].

145. Makena Kelly, *All the Ways Congress is Taking on the Tech Industry*, VERGE (Mar. 3, 2020, 9:20AM), https://www.theverge.com/2020/3/3/21153117/congress-tech-regulation-privacy-bill-coppa-ads-laws-legislators [https://perma.cc/CEW5-P2ME] ("Warner's ACCESS Act would, if approved, require big tech companies like Facebook and Google to build more open APIs that allow data sharing with smaller competitors. It would force these companies to maintain interfaces that facilitate the "secure transfer of user data" to users and competing services.").

146. Massimo Russo, David Young, Tian Feng & Marine Gerard, *Sharing Data to Address Our Biggest Societal Challenges*, BCG HENDERSON INST. (Jan. 7, 2021), https://www.bcg.com/publications/2021/data-sharing-will-be-vital-to-societal-changes [https://perma.cc/7PT3-ECAR] (explaining the many opportunities for using AI for social good); *see, e.g.*, Chakravortl, *supra* note 1; Nenad Tomašev, Julien Cornebise, Frank Hutte, Shakir Mohamed, Angela Picciariello, Bec Connelly, Danielle C. M. Belgrave, Daphne Ezer, Fanny Cachat van der Haert, Frank Mugisha, Gerald Abila, Hiromi Arai, Hisham Almiraat, Julia Proskurnia, Kyle Snyder, Mihoko Otake-Matsuura, Mustafa Othman, Tobias Glasmachers, Wilfried de Wever, Yee Whye Teh, Mohammad Emtiyaz Khan, Ruben De Winne, Tom Schaul & Claudia Clopath, *AI for Social Good: Unlocking the Opportunity for Positive Impact*, NATURE COMMS. (2020), https://www.nature.com/articles/s41467-020-15871-z.pdf [https://perma.cc/VZ8S-YBY3] ("Amnesty International and Element AI demonstrated how AI can be used to help trained human moderators with identifying and quantifying online abuse against women on Twitter. The Makerere University AI research group supported by the UN Pulse Lab Kampala developed automated monitoring of viral cassava disease, and this same group collaborated with Microsoft Research and other academic institutions to set up an electronic agricultural marketplace in Uganda. Satellite imagery was used to help predict poverty and identify burned-down villages in conflict zones in Darfur, and collaborative efforts between climate and machine learning scientists initiated the field of climate informatics that continues to advance predictive and interpretive tools for climate action." (citations omitted)).

147. Martens, *supra* note 14.

148. *See id.*

149. Cesare Fracassi & William J. Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 330 (2021) ("[O]ne of the core goals of financial regulation is to encourage, and in some cases require, the disclosure of useful information in order to make markets fairer and more efficient. Data

both commercial activity that data brokers readily supply with data, as well as the strategic activities of not-for-profits and non-governmental organizations.[150] With a much more constrained flow of new data into the latter, there is reduced use for social good than if such data were more equally accessible.[151]

However, public entities hold far less of this valuable data when compared with the private industry.[152] Even the growing government data troves are commonly reformatted for sale as a "value added" activity by most data brokers.[153] The potential for identifying and responding to natural disasters, identifying and tracking endangered animals, detecting pathologies, and managing scarce resources,[154] for example, lies in AI and the ability to access and analyze this data.[155] However, there are enormous disincentives for Big Tech to share their collected data or develop applications for social good.[156] First, the data held by Big Tech provides them with an enormous competitive advantage.[157] Second, companies could put themselves at risk for potential data breaches if they share data with unreliable partners.[158]

---

sharing, thus, is a tremendously powerful tool for social good." (citations omitted)); *see also* Houser, *Artificial Intelligence, supra* note 77, at 486–492.

150. *See generally* Alberto Alemanno, *Data for Good: Unlocking Privately-Held Data to the Benefit of the Many*, 9 EUR. J. RISK REGUL. 2, 2–4 (2018); *Data Science for Non-profits,* DISCOVER DATA SCI., https://www.discoverdatascience.org/social-good/nonprofits/ [https://perma.cc/S8SC-WYZF] (last visited Nov. 4, 2022).

151. *See* Alemanno, *supra* note 150, at 1, 10.

152. *Id.* at 2.

153. Lexis-Nexis and Westlaw are paradigms of large data brokerages acquiring the majority of their data from government sources. *See generally* CAREY SHENKMAN, SHARON BRADFORD FRANKLIN, GREG NOJEIM & DHANARAJ THAKUR, LEGAL LOOPHOLES AND DATA FOR DOLLARS: HOW LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE BUYING YOUR DATA FROM BROKERS 10, 33 (2021) https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf [https://perma.cc/2AD7-FQPA].

154. Houser, *Artificial Intelligence*, *supra* note 77, at 486, 488, 490.

155. *Id.* at 475.

156. *See* STEFAAN G. VERHULST, ANDREW YOUNG, ANDREW J. ZAHURANEC, SUSAN ARIEL AARONSON, ANIA CALDERON, AND MATT GEE, THE EMERGENCE OF A THIRD WAVE OF OPEN DATA: HOW TO ACCELERATE THE RE-USE OF DATA FOR PUBLIC INTEREST PURPOSES WHILE ENSURING DATA RIGHTS AND COMMUNITY FLOURISHING 22–23 (2020), https://ssrn.com/abstract=3937638 [https://perma.cc/89Q8-GNSJ] (explaining that even if private actors wanted to share their data for public good (and some do), the lack of regulatory guidance inhibits them from doing so).

157. *See, e.g.*, Andrei Hagiu & Julian Wright, *When Data Creates Competitive Advantage*, HARV. BUS. REV. (2020), https://hbr.org/2020/01/when-data-creates-competitive-advantage [https://perma.cc/8372-CQXW].

158. *See Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business [https://perma.cc/2R9P-AT7K]. *See generally* Sara Rouhani & Ralph Deters, *Data Trust*

Third, publicly held companies have a duty to their shareholders, which requires the maintenance of their competitive advantage over sharing for social good.[159] Unlike in the European Union, where funding to develop technology is primarily sourced from the government,[160] private industry funds most technological advances in the United States.[161] In the United States, most AI technology development results from commercial investment in hoped-for money-making endeavors.[162] There is little incentive for Big Tech to develop AI primarily for social good.[163]

However, even if businesses wanted to share data—and according to a report in the Harvard Business Review, 66 percent of companies surveyed do—"strict regulatory oversight applies to certain private data, with violations risking significant costs financially and to reputations."[164] Overall, the harms briefly described in this Part result from the misallocation of data by Big Tech, which includes both oversharing (harm to data subjects) and under-sharing (harm to SMEs and organizations seeking to use data for social good).[165] While the European Union has long sought to limit Big Tech from treating personal data as a good to be manipulated through antitrust action[166] and increasingly strict privacy regulations,[167] the United States has

---

*Framework Using Blockchain Technology and Adaptive Transaction Validation*, 9 IEEE ACCESS 90379, 90379 (2021) (proposing "an end-to-end framework for data trust to enhance trustworthy data sharing utilizing blockchain technology").

159. *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 503–04 (2019).

160. *See* European Commission Press Release IP/22/2843, Commission Boosts Horizon Europe Budget to Support Green, Health and Digital Innovations and Displaced Researchers of Ukraine (May 10, 2022).

161. Kimberly A. Houser, *The Innovation Winter Is Coming: How the U.S.-China Trade War Endangers the World*, 57 SAN DIEGO L. REV. 549, 552 (2020).

162. *Id.* at 602 (explaining "advancements in AI in the United States have been funded and guided primarily by private industry advancing commercial pursuits").

163. Kate Jones, Marjorie Buchser & Jon Wallace, *Challenges of AI*, CHATHAM HOUSE (Mar. 22, 2022), https://www.chathamhouse.org/2022/03/challenges-ai [https://perma.cc/SP47-D9YB].

164. George Zarkadakis, *"Data Trusts" Could Be the Key to Better AI,* HARV. BUS. REV (Nov. 10, 2020), https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai [https://perma.cc/L9LE-276Y].

165. Stefan Mager & Johann Kranz, *Stimulating Economic Growth by Unlocking the Nonrival Potential of Data - Review, Synthesis and Directions for Future Research* 1 (Ludwig Maximilian U. Working Paper, Paper No. 02, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3720114 [https://perma.cc/86RF-U5K9] (describing the potential for individual and societal harms due to big data misallocation, despite its potential for innovation and economic growth).

166. *See* Stucke, *supra* note 15.

167. *Data Protection Under GDPR*, EUROPA, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm [https://perma.cc/FBB7-J2YD] (Jun. 7, 2022); *see also* Houser & Voss, *supra* note 37, at ¶ 116.

only recently begun to take this route.[168] Currently, forty-six states and the Federal Trade Commission have brought actions against Facebook,[169] and thirty-eight states and the Justice Department have brought actions against Google.[170] In the United States, while some have encouraged breaking up Big Tech,[171] others have called for GDPR-type regulations.[172] There is an immense difference in ideology around privacy in the European Union and United States.[173] Under EU law, privacy is a fundamental right,[174] while there is no mention of privacy in the US Constitution.[175] These differences (and the failure of

168. *See* Chakravortl*, supra* note 1 ("Despite AI's growing importance, [US] policy on how to manage the technology is fragmented and lacks a unified vision. It also appears to be an afterthought, with lawmakers more focused on Big Tech's anticompetitive behavior in its main markets—from search to social media to app stores.").

169. However, the antitrust actions against Facebook have been dismissed in forty of the states. Cecilia Kang, *Judge Throws Out 2 Antitrust Cases Against Facebook*, N.Y. TIMES (Oct. 4, 2021), https://www.nytimes.com/2021/06/28/technology/facebook-ftc-lawsuit.html [https://perma.cc/6J5F-GJZG]. On January 11, 2022, a federal judge denied Facebook's motion to dismiss the FTC's antitrust action against them. Brent Kendall, *Federal Judge Rejects Facebook's Request to Dismiss FTC's Latest Antitrust Lawsuit*, WALL ST. J. (Jan. 11, 2022, 5:10 PM ET), https://www.wsj.com/articles/federal-judge-rejects-facebooks-request-to-dismiss-ftcs-latest-antitrust-lawsuit-11641932982 [https://perma.cc/QV5Y-83TJ] (regarding a suit alleging that Facebook abuses its market power in social media).

170. John D. McKinnon, *These Are the U.S. Antitrust Cases Facing Google, Facebook and Others*, WALL ST. J. (Dec. 17, 2020, 3:17 PM), https://www.wsj.com/articles/these-are-the-u-s-antitrust-cases-facing-google-facebook-and-others-11608150564 [https://perma.cc/TH93-3BV7].

171. *See* Robert Fay, Blayne Haggart & Natasha Tusikov, *Reining in Big Tech: Is This the End of the Beginning?,* CTR. FOR INT'L GOVERNANCE INNOVATION (July 23, 2021), https://www.cigionline.org/articles/reining-in-big-tech-is-this-the-end-of-the-beginning/ [https://perma.cc/2KFW-C5E9] (discussing recent bills coming out of the US House committee on the Judiciary); *see also* Eleanor M. Fox & Harry First, *We Need Rules to Rein in Big Tech*, CPI ANTITRUST CHRONICLE, Oct. 2020, no. 2, AT 25, 26 (proposing antitrust rulemaking by the FTC).

172. *See* Michele E. Gilman, *Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice*, 52 ARIZ. ST. L.J. 368, 373–74 (2020).

173. *See* Houser & Voss *supra* note 37, at ¶ 115 (detailing the differences between the United States and European Union in privacy and data protection doctrine).

174. Charter of Fundamental Rights of the European Union art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 10.

175. *See* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2245 (2022). The United States and European Union have fundamentally different approaches to privacy, perhaps even based on an elusive ideology. In the United States, privacy protection is sectoral (narrowly applicable) and apparently, following *Dobbs*, may no longer be considered a right under either textual or implied interpretations of the US Constitution. By contrast, in the European Union, privacy is omnibus (broadly applicable) and is a sturdy, fundamental right because it is explicitly stated in the EU constitution and is again and again implemented in the laws and regulations of all member states. *See* Houser & Voss, *supra* note 37, at ¶¶ 18–19. *See generally* Dobbs, 142 S. Ct. 2228. On September 2, 2021, the US Supreme Court took the first step towards eviscerating privacy rights in *Whole Woman's Health v. Jackson*, 142 S. Ct. 522 (2021). *In Dobbs v. Jackson Women's Health Organization*, 142 S. Ct. 2228 (2022), the Court went further in eliminating

the United States to meet the privacy "adequacy" standard under the GDPR) resulted in the invalidation of the Privacy Shield, which previously permitted data transfers from the European Union to companies in the United States.[176] Although there appears to be global agreement that something must be done to rein in Big Tech, governments do not agree on answers.[177]

## III. DATA SHARING MODELS

There is an enormous power imbalance from the consolidation of control into just a handful of massive data brokerage companies.[178] Moreover, data firms consistently struggle to balance multiple divergent stakeholder objectives.[179] In order to balance the sharing of data for commercial purposes, academic use, and social good with the preservation of privacy and prevention of individual and collective harms, a number of models have emerged, ranging from personal data sovereignty[180] to forced data sharing.[181] Between these two extremes lie

---

privacy rights that had been explained in *Roe v. Wade*, 410 U.S. 113 (1973). Privacy rights are very fragile in the United States. The European Union understands this, which is why the United States fails to meet the "adequacy" standard required by the European Union regarding personal data transfers. *See* ARCHICK & FEFER, *supra* note 107. The Authors expect a further narrowing of privacy rights due to the conservative majority on the current Supreme Court.

176. ARCHICK & FEFER, *supra* note 107. In addition, calls for global harmonization of privacy law or agreement on the reigning in of Big Tech are not likely to be answered. In fact, according to the New York Times, "while governments agree that tech clout has grown too expansive, there has been little coordination on solutions. Competing policies have led to geopolitical friction." Paul Mozur, Cecilia Kang, Adam Satariano & David McCabe, *A Global Tipping Point for Reining in Tech Has Arrived*, N.Y. TIMES (Apr. 30, 2021), https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html [https://perma.cc/4LX7-HYS5].

177. Swabey & Harracá, *supra* note 128 (explaining that world governments are wrestling with how to regulate Big Tech).

178. Angelina Fisher & Thomas Streinz, *Confronting Data Inequality*, 60 COLUM. J. TRANSNAT'L L. 829, 835 (2022) (advocating for "[s]maller, local but also potentially transnationally aligned actors could be empowered to make their own choices about which data to collect and how and which data infrastructures to use and to rely on").

179. *See infra* note 182 and accompanying text.

180. *See* Jan J. Zygmuntowski, Laura Zoboli & Paul F. Nemitz, *Embedding European Values in Data Governance: A Case for Public Data Commons*, 10 INTERNET POL'Y REV., no. 3, 2021, at 5, 7 (personal data sovereignty considers data subjects to be the owners of their data with the ability to sell it).

181. Frederik Claessens, *The End of the "Wild West": How the Digital Markets Act Will Transform Digital Services*, SQLI DIGIT. EXPERIENCE (Nov. 9, 2021), https://www.sqli.com/int-en/insights-news/blog/end-wild-west-how-digital-markets-act-will-transform-digital-services [https://perma.cc/ZU99-8AQF] ("In concrete terms, the [European Union's DMA] will force gatekeepers to open access to their services (interoperability), to transmit end-user data to companies (data sharing) and ultimately allow third-party companies to enter into contracts and pursue business relationships outside of the systemic platforms."). It has also been suggested that

data governance structures.[182] The original concept of governance structures, known as "commons," stems from Nobel laureate Elinor Ostrom's 1990 seminal work, *Governing the Commons.*[183]

Although the concept is difficult to define, a commons is understood as any natural or man-made resource that is or could be held and used in common.[184] The International Association for the Study of the Commons, for example, "is devoted to bringing together interdisciplinary researchers, practitioners, and policymakers for the purpose of fostering better understandings, improvements, and sustainable solutions for environmental, electronic, and any other type of shared resource that is a commons or a commons-pool resource."[185]

Investigating communities around bodies of water, Elinor Ostrom discovered that these communities often found ways to share by creating their own rules.[186] This was counter to the idea that people would behave selfishly and use up common resources without top-down regulations.[187] Through years of research, Elinor Ostrom concluded that

---

fiduciary duties be imposed on Big Tech. *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment,* 49 U.C. DAVIS L. REV. 1183, 1186 (2016). *But see* Khan & Pozen, *supra* note 159, at 498 (responding to Balkin's information fiduciary model and suggesting that this would violate corporate law, which holds that corporations have a duty of loyalty to their shareholders and as such could not serve as information fiduciaries to data subjects).

182. *See generally* Zygmuntowski et al., *supra* note 180. As with trade-secret-protected information, ownership standing alone does not preclude the rightful use of data by others, such as through mass-market licensing. Furthermore, a party's assertion of ownership over information in the public domain may constitute a viable legal claim if uniquely selected and arranged, essentially organized as a value-added enhancement by intermediaries such as data brokers. *See, e.g.*, Feist Publ'ns, Inc., v. Rural Tel. Serv. Co., 499 U.S. 340 (1991). *See generally Frequently Asked Questions: Trade Secrets*, WIPO, https://www.wipo.int/tradesecrets/en/tradesecrets_faqs.html [https://perma.cc/U59U-UH28] (last visited Nov. 4, 2022). Data governance structures would permit data subjects to have a voice in the use of their data, arguably overriding ownership, licensing, or other allegedly rightful uses of the data. *See generally Participatory Data Governance*, ADA LOVELACE INST., https://www.adalovelaceinstitute.org/project/participatory-data-governance/ [https://perma.cc/E6JA-RKUJ] (last visited Nov. 4, 2022).

183. *See generally* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990).

184. *See* Shkabatur, *supra* note 40, at 411 n. 113; *see also About the Commons*, INT'L ASS'N FOR STUDY OF COMMONS, https://iasc-commons.org/about-commons/ [https://perma.cc/3QKV-C4TE] (last visited Nov. 4, 2022).

185. *ISAC's Goals*, INT'L ASS'N FOR STUDY OF COMMONS, https://iasc-commons.org/goals/ [https://perma.cc/KG25-XVVB] (last visited Nov. 14, 2022).

186. Anouk Ruhaak, *Data Commons and Data Trusts*, MEDIUM (May 15, 2020), https://medium.com/@anoukruhaak/data-commons-data-trust-63ac64c1c0c2 [https://perma.cc/Q7RK-Q8YK] (noting, with respect to common pool resources, that "[Ostrom's] research found that communities often find ways to decide on access to and use of the resource between themselves").

187. *Elinor Ostrom – The "Non-Tragedy of the Commons,"* CGIAR WATER, LAND & ECOSYSTEMS, https://wle.cgiar.org/news/elinor-ostrom-%E2%80%9Cnon-tragedy-commons%E2%80%9D [https://perma.cc/86KY-RK85] (last visited Nov. 4, 2022). This concept, known

not only were groups capable on their own to avoid the tragedy of the commons, but that top-down regulation was not required or even beneficial.[188]

The commons concept has also been applied in the literature to data writ large.[189] In essence, a "data commons" is a collection of data that is shared as a common resource.[190] By combining their data, a group of individuals can obtain better bargaining leverage for the use of their data.[191] The grouping of this data can address the power imbalance between data subjects and corporate data controllers.[192] As Oliver E. Williamson argues,[193] for innovative governance models such as data trusts,[194] "governance provides a framework for establishing accountability, roles, and decision-making authority from an organization."[195] The success of this governance model requires a "clear

---

as the *tragedy of the commons*, was coined by ecologist Garrett Hardin and described the idea that "people thinking only of their own self-interest, deplete a shared resource, e.g., the overgrazing of pastures. He saw two solutions to this problem; 1) resource regulation through government intervention and 2) privatization." *Id*.

188. OSTROM, *supra* note 183, at 1 and 58. The Ostrom study involved Switzerland, Spain, the Philippines, and Japan. *Id*.

189. *See* BRETT M. FRISCHMANN, MICHAEL MADISON & KATHERINE J. STANDBURG, GOVERNING KNOWLEDGE COMMONS 1–2 (2014) (explaining that although data is not a common pool resource, it does share characteristics in that certain parties may be able to legally exclude others from accessing the data).

190. Jonathan van Geuns & Ana Brandusescu, *What Does it Mean? | Shifting Power Through Data Governance*, MOZILLA FOUND. (Sept. 16, 2020), https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/ [https://perma.cc/8LGT-AJDG].

191. *See id.*

192. *See id*.

193. See Adam Smith, *Transcript from an Interview with Elinor Ostrom and Oliver E. Williamson*, NOBEL PRIZE (Dec. 6, 2009), https://www.nobelprize.org/prizes/economic-sciences/2009/ostrom/164465-ostrom-williamson-interview-transcript/ [https://perma.cc/B9DW-KKBE].

194. *See* Oliver Williamson, *The Economics of Governance*, 95 AM. ECON. REV. 1, 1 (2005); *The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2009*, NOBEL PRIZE (Dec. 2009), https://www.nobelprize.org/prizes/economic-sciences/2009/summary/ [https://perma.cc/7F2Y-HSWV]. Ostrom and Williamson shared the Nobel prize for their independent contributions to economic governance. *See id.*

195. Kevin Werbach, *The Siren Song: Algorithmic Governance By Blockchain*, *in* AFTER THE DIGITAL TORNADO: NETWORKS, ALGORITHMS, HUMANITY 215 (Kevin Warbach ed., 2020); *Oliver E. Williamson – Facts*, NOBEL PRIZE, https://www.nobelprize.org/prizes/economic-sciences/2009/williamson/facts/ [https://perma.cc/T683-XSFN] (last visited Nov. 4, 2022). Williamson describes the baseline for what data governance is seeking to accomplish—a decision-making framework. Williamson's thesis is that there is a way to determine whether a transaction should take place within a firm or the marketplace. "Financial analysis has most often focused on markets, whereas Oliver Williamson's research concentrates more on organizations. According to Oliver Williamson, markets and companies used different conflict

definition of the contents of the common pool resource and effective exclusion of external un-entitled parties."[196] The following Sections discuss various data-sharing models that might achieve such governance success, including data pools and cooperatives, corporate and contractual mechanisms, and data trusts.[197]

### *A. Data Cooperatives and Data Pools*

When a group voluntarily pools their data together, this is known as a data cooperative or data pool.[198] Cooperatives and pools are based on the idea that data as a collective provides more bargaining power than an individual data subject would have.[199] The main difference between a data cooperative and a data pool is the structure.[200] A data cooperative manages the data on behalf of the participants, and a data pool permits all participants to participate in the management.[201]

One example of a data cooperative is Driver's Seat, which combines driver data from contractor drivers (like Uber and Lyft) to be able to make use of its own data, rather than the company maintaining sole control.[202] The cooperative can then monetize the data by selling it to city agencies.[203] An example of a shared data pool is the traffic app Waze, which shares traffic information with municipalities in exchange for information on road closings and road construction.[204] The main disadvantage to this form of data governance model is that it excludes the data subjects—the drivers—from determining how these entities use their data.[205]

A data cooperative is a more democratic model.[206] One example is the MIDATA.coop, which permits data subjects to share their

---

resolution methods. In the early 1970s, he proposed the theory that organizations are sometimes more efficient than markets because their conflicts are simple and cheaper to solve." *See Oliver E. Williamson – Facts*, *supra*; *Williamson*, *supra* note 194, at 1–2.

196. Ruhaak, *supra* note 186; OSTROM, *supra* note 183, at 190.

197. *See infra* Section III.A.

198. *See* van Geuns & Brandusescu, *supra* note 190.

199. *See id.*

200. *See id.*

201. *See id.*

202. *Id.*

203. *See id.*

204. Marina Micheli, Marisa Ponti, Max Craglia and Anna Berti Suman, *Emerging Models of Data Governance in the Age of Datafication*, 7 BIG DATA & SOCIETY, 2020, at 7, https://journals.sagepub.com/doi/10.1177/2053951720948087 [https://perma.cc/9BAD-NT78].

205. *See id.*

206. *See id.*

personal health information for research purposes.[207] The main issue with this cooperative is that for the data subject to gain the benefit from sharing their data to receive accurate information about their condition, a personal identifier is connected to their personal health information, raising privacy concerns.[208] Data cooperatives have several disadvantages: they need financing to perform their obligations and may lack a sufficient number of participants to interest data users.[209] Data pools, because of their democratic nature, may find it difficult to make decisions when there are many members.[210] In addition, both of these structures are informal, making them unlikely to address the potential costs in data collection, preparation, and compliance.[211] Data pools and cooperatives lack the more formal ownership transfers and fiduciary duties of the trustee as intermediary discussed below.

### *B. Corporate and Contractual Mechanisms*

When organizations seek to share data with or between one another, they can either engage directly using a contractual mechanism or indirectly through a third-party corporate mechanism.[212] The corporate model requires the interposition of a separate legal entity to serve as an intermediary.[213] Data sharing agreements can also be negotiated between businesses and governments.[214] Although there have been some one-off agreements, in general, there are significant barriers to such arrangements, including: "(a) monopolistic data markets, (b) high transaction costs and perceived risks in data sharing and (c) a lack of incentives for private firms to contribute to the production of public benefits."[215] Both of these mechanisms are very

207. *Id*.

208. *See* Ilse van Roessel, Matthias Reumann & Angela Brand, *Potentials and Challenges of the Health Data Cooperative Model*, 20 PUB. HEALTH GENOMICS 321, 327 (2018).

209. *See* ADA LOVELACE INST. & U.K. A.I. COUNCIL, EXPLORING LEGAL MECHANISMS FOR DATA STEWARDSHIP 65 (2021), https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/ [https://perma.cc/AF5Z-3DQV].

210. *See* van Geuns & Brandusescu, *supra* note 190.

211. *See* ADA LOVELACE INST. & U.K. A.I. COUNCIL, *supra* note 209, at 6–7, 54.

212. *See id.*

213. *See id.* at 7.

214. *See* van Geuns & Brandusescu, *supra* note 190.

215. *See* BERTIN MATINS & NESTOR DUCH-BROWN, THE ECONOMICS OF BUSINESS-TO-GOVERNMENT DATA SHARING, JR TECHNICAL REPORT, EUROPEAN COMMISSION 5 (2020).

limited in scope and do not provide much flexibility.[216] As such, they are inappropriate to address the complex issues in data governance.[217]

The main disadvantage to corporate and contractual mechanisms is that governance is not the primary objective.[218] Rather, the purpose of such corporate and contractual mechanisms is to facilitate data sharing between a limited number of partners and ensuring the interoperability of the data.[219] In addition, in many cases the parties to the mechanisms do not obtain specific consent from the data subjects for the sharing of this data.[220] These types of arrangements primarily benefit private entities, although they may provide access or compensation to the data subjects.[221] The extent of data governance and protection depends on what terms are negotiated, as there is no fiduciary duty owed to the data subjects under contract law.[222] In fact, the duty of good faith and fair dealing implied in contracting is fairly limited.[223] Indeed, contract law demands no more than "*minima moralia* of the marketplace," a far weaker duty than that of a fiduciary.[224] As such, corporate and contractual mechanisms lack the fiduciary stewardship necessary to protect the data subjects, nor is anything other than a basic duty of good faith imposed on the private entities with respect to the use of the shared data.[225]

---

216. *See* ADA LOVELACE INSTITUTE & U.K. A.I. COUNCIL, *supra* note 209, at 69–74 (suggesting that the corporate model may provide a degree more flexibility than the contractual model).

217. *See id.* at 74.

218. *See id.*

219. *See id.* at 70, 72.

220. *See id.* at 32.

221. *See id.* at 74–75.

222. *See id.* at 73–74; *supra* note 181 and accompanying text. *Compare Data Use and Non-Disclosure Agreement Concerning the Disclosure of Data for Michigan's Trauma Registry*, MICH. (July 9, 2015), https://www.michigan.gov/documents/mdch/Data_Use_and_Non_Disclosure_Data_Disclosed_to_MDCH_Trauma_Registry_Final_465518_7.pdf [https://perma.cc/5PZA-P3MP], *with Master Data Sharing Agreement*, CAMDEN COAL. HEALTHCARE PROVIDERS (May 1, 2017), https://www.nationalcomplex.care/wp-content/uploads/2018/06/Appendix-B-Data-Sharing-Agreement-Template.pdf [https://perma.cc/ER26-ZLXM] (providing an example of the different levels of protection offered by data sharing agreements).

223. *See* RESTATEMENT (SECOND) OF CONTRACTS, § 205 (AM. L. INST. 2015) ("Every contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement.").

224. GREGORY KLASS, *What If Fiduciary Obligations Are Like Contractual Ones? in* CONTRACTS, STATUS, AND FIDUCIARY LAW 93, 96 (Paul B. Miller & Andrew S. Gold, eds., 2016).

225. *See id.*; RESTATEMENT (SECOND) OF CONTRACTS, § 205 (AM. L. INST. 2015).

### *C. Data Trusts*

A data trust is the most formal of all models, but it may best address the inadequacy of both regulations and contract law.[226] The term "data trust" as used herein refers to a governance model for data sharing that could be configured as a legal trust under trust law.[227] One of the benefits of a data trust is that the data subjects can aggregate their rights to provide more bargaining power with data users and control over the use of their data.[228] In addition, it can leverage existing trust law and instill fiduciary duties in the intermediary between the data subjects and data users to address the data sharing problems discussed in Part II.[229]

A data trust can provide both a voice and protection for data subjects through the use of a trust structure with a fiduciary trustee entrusted to negotiate on behalf of the subjects with third parties.[230] This mechanism can more directly provide adequate data governance than the contractual or corporate examples just discussed.[231] In addition, data trusts can be structured to provide the flexibility to hold different types of data for different purposes.[232] This approach provides the most functionality of all of the models. A trust could act on behalf of a large group of data subjects, exercise their data rights, protect the data from harm, and permit use by businesses who would not otherwise have access to such data as well as by researchers seeking to promote

---

226. *See* John T. Holden & Kimberly A. Houser, *Taboo Transactions: Selling Athlete Biometric Data*, 49 FLA. ST. U. L. REV. 103, 152 (2022).

227. There is some disagreement in the data trust community as to whether a data trust can be created under trust law. First, some argue data should not constitute property and thus cannot be held in a trust. Second, many jurisdictions do not recognize trusts. Third, the data trust envisioned herein considers the needs of all stakeholders, which would include the data users in addition to the data subjects, which would constitute a conflict of interest under traditional trust law. Another potential conflict would be with a board of trustees that includes beneficiaries. *See* Delacroix & Lawrence, *supra* note 24 at 241, 244–45; Michael W. Galligan, *United States Trust Law and the Hague Convention on Trusts*, TR. & EST. L. SECTION NEWSLETTER (N.Y. State Bar Ass'n, Albany N.Y.), Fall 2000, at 37; *see also* SOPHIE STALLA-BOURDILLON, ALEXSIS WINTOUR & LAURA CARMICHAEL, BUILDING TRUST THROUGH DATA FOUNDATIONS 4–20 (2019) (suggesting that foundation law (as distinct from contract or trust law) in the Channel Islands would provide an existing framework for data trusts).

228. *See* Delacroix & Lawrence, *supra* note 24, at 236–242; Keith Porcaro, *In Trust, Data*, 105 MINN. L. REV. HEADNOTES 332, 337 (2021).

229. *See* Delacroix & Lawrence, *supra* note 24, at 240.

230. *See id.* at 236. This Article uses the term "trustee," singular, to represent a single trustee or board of trustees.

231. *See id.*

232. *See infra* Part IV; *see also* ELEMENT AI & NESTA, DATA TRUSTS: A NEW TOOL FOR DATA GOVERNANCE 14–15 (2019), https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf [https://perma.cc/E534-Q298].

social good.[233] Additionally, data trusts can be tailored to the specific types of data or needs of the data subjects.[234] Currently, multiple test cases are being conducted that will inform later developments.[235] The following Section explains how data trusts work and why they could offer the best solution to the issues noted in Part II.

## IV. DATA TRUST SOLUTION

Trusts originated in English-speaking nations under equity, the separate branch of common law developed in the ecclesiastical English courts of Chancery.[236] Chancery courts flourished during medieval times as a mechanism to mitigate rigidity in the rule of law.[237] Equity recognized the utility of trusts when the best interests represented by property ownership diverged from the rights of that property's beneficiary.[238]

---

233. *See* SYLVIE DELACROIX & JESSICA MONTGOMERY, FROM RESEARCH DATA ETHICS PRINCIPLES TO PRACTICE: DATA TRUSTS AS A GOVERNANCE TOOL 8–9 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3736090 [https://perma.cc/KE4S-PE4D]; *see also* GLOB. P'SHIP ON A.I., ENABLING DATA SHARING FOR SOCIAL BENEFIT THROUGH DATA TRUSTS: DATA TRUSTS IN CLIMATE 14–25 (2022), https://gpai.ai/projects/data-governance/data-trusts/ [https://perma.cc/3NAQ-7QEQ] (there is currently a pilot project in the United Kingdom to support using data trust for social good).

234. *See* Delacroix & Lawrence, *supra* note 24, at 243; *see also, e.g.*, P. Alison Paprica, Eric Sutherland, Andrea Smith, Michael Brudno, Rosario G. Cartagena, Monique Crichlow, Brian K. Courtney, Chris Loken, Kimberlyn M. McGrail, Alex Ryan, Michael J. Schull, Adrian Thorogood, Carl Virtanen & Kathleen Yang, *Essential Requirements for Establishing and Operating Data Trusts*, 5 INT'L J. POPULATION DATA SCI., no. 1, 2020, at 2–3 (providing minimum specifications for a public data trust for health data under Canadian law).

235. *See*, *e.g.,* Stefan Baack & Madeleine Maxewell, *Who Is Innovating? | Global Landscape Scan and Analysis of Initiatives*, MOZILLA FOUND. (Sept. 16, 2020), https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/whos-trying-global-landscape-scan-and-analysis/, [https://perma.cc/8FK4-VTPU]; *Data Trusts: Lessons from Three Pilots*, *supra* note 29 (listing a range of projects).

236. *See generally* Ugo Mattei & Henry Hansmann, *Trust Law in the United States. A Basic Study of Its Special Contribution*, 46 AM. J. COMP. L. SUPP. 133, 134 (1998) (expanding on the origins of trust law, with a focus on the historical path followed by English law).

237. *See, e.g.*, *id.* (emphasizing that equity courts created a stable system of trust law, allowing the beneficiary their rights to their property despite the trustee being the owner at law).

238. *See id.* For example, the early English trusts protected Crusaders' landholdings when conveyed to others during the Crusaders' Holy Land pilgrimages. Too frequently, trustees defaulted on their fiduciary promises to re-convey lands back to returning Crusaders many years later. Equity enforced these medieval trustees' original promises. Voluminous citable primary resources exist for the impact that the eleventh to thirteenth Century Crusades has had on modern commercial practices; the sources themselves constitute big data. *See generally How the Crusades Created Estate Planning*, SHEPPARD L. FIRM (June 16, 2020), https://www.sbshlaw.com/how-the-crusades-created-estate-planning/ [https://perma.cc/ZNU2-VWRT]. *But see* Irina Gvelesiani, *The Roman Origin of the Trust (Juridicial-Linguistic Peculiarities)*, 26 TRUSTS & TRUSTEES 907, 908 (2020).

In the most common trust formulation, there are three parties involved.[239] A trustor initiates the trust by transferring property to the trustee, who manages the property on behalf of the beneficiary.[240] The trustee holds legal title to the property (trust res), and the beneficiary holds equitable ownership rights to the property.[241] This bifurcation gives rise to the fiduciary duties of the trustee.[242] Trustees are bound to fiduciary duties of prudence and loyalty as reinforced, enumerated, or modified by trust agreement provisions that either benefit the beneficiary or relax fiduciary duties.[243]

Most testing of data trusts is occurring outside of the United States.[244] However, one notable exception is the Willis Tower Watson (WTW) data trust pilot.[245] The WTW was developed as a prototype to identify a business case and form a successful minimal viable consortium that satisfied legal and ethical constraints and allowed data sharing by exploring various enabling technologies.[246] This format provides ethical governance of data by assuring individual subjects' assent to data uses, the removal of data biases, and the anonymization of the data.[247]

The Authors anticipate that data trusts will eventually be understood as a big data design or big data architecture.[248] That is, successful data trusts operating in the near to medium-term future will likely be algorithm-driven to operate efficiently and effectively by deploying economies of scale.[249] Otherwise, human-mediated transaction costs most certainly would relegate data trusts to the

239. *See* Mattei & Hansmann, *supra* note 236.

240. *See id.*

241. *See id.*

242. ROBERT SITKOFF, *Fiduciary Principles in Trust Law*, *in* OXFORD HANDBOOK OF FIDUCIARY LAW, 41, 42 (2019).

243. *See id.* at 43–60.

244. *See* Zarkadakis, *supra* note 164.

245. *See id.*

246. *See id*. *See generally* van Geuns & Brandusescu, *supra* note 190 (there are a number of nonprofit, governmental, and university research groups exploring the use of data trusts, primarily with respect to public data, such as the Open Data Institute in the United Kingdom and the Aapti Institute in India).

247. *See* Zarkadakis, *supra* note 164.

248. *Big Data Architecture Style,* MICROSOFT, https://learn.microsoft.com/en-us/azure/architecture/guide/architecture-styles/big-data [https://perma.cc/U5NQ-U494] (last visited Nov. 5, 2022) (explaining that big data design (also known as big data architecture) is the method by which data is ingested, processed, and analyzed).

249. *See, e.g.*, *id.* (describing big data architecture, including the benefits, challenges, and best practices).

rarified "private banking"-style costs of administration.[250] The function of data trusts proposed by most innovators is to address the hugely voluminous subject matter res.[251] The most hopeful vision of achieving success in data trust deployment involves a simple model, emphasizing a mostly effortless migration to fiduciary control and custody. However, critics predict much more complexity, likely derived from their expectations for dependence on a prodigious maze of privacy enablement statutes, interjurisdictional enforceability compacts, and any predictable, misplaced reliance on strong technical controls over fugacious information.[252]

Information economics recognizes that tight security over information of any type is quite challenging.[253] First, most forms of information can be classified as intangible property;[254] second, much information is non-rival and inexhaustible;[255] and third, much information is very valuable.[256]

These axioms are consistent with the concession that PII should be a form of intellectual property (IP), enabling exploitation by its

---

250. *See,* e.*g.,* Casey Bond, *Is Private Banking Right for You?*, U.S. NEWS & WORLD REP. (Feb. 15, 2022, 12:22 PM), https://money.usnews.com/banking/articles/is-private-banking-right-for-you [https://perma.cc/MTT9-PHUB] (stating that private banking cannot achieve the same economies of scale as regular consumer banking).

251. *See* Xiaosong Zhang, *A Commentary of Data Trusts in MIT Technology Review 2021*, 6 FUNDAMENTAL RSCH. 834, 834 (2021) (describing data trusts as a new concept in big data).

252. *See, e.g.*, Lisa M. Austin & David Lie, *Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust*, 19 SURVEILLANCE & SOC'Y 255, 259–60 (2021).

253. *See, e.g.*, Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCI. 610 (2006) (arguing numerous security market failures dictate information security failure, including misaligned incentives, network insecurity as a negative externality, failure of products in the market for securing private data, and incentives to price discriminate in the sale of private data); Ross Anderson, *Why Information Security is Hard – An Economic Perspective*, PROCEEDINGS 17TH ANN. COMPUT. SEC. APPLICATIONS CONF., 358–365 (2001), https://www.acsac.org/2001/papers/110.pdf [https://perma.cc/Y4GK-G9LL] (listing a considerable amount of literature addressing the difficulties and costs of security for various types of information). *See generally* John W. Bagby, *Security Law, Regulation and Public Policy for Accounting Professionals,* SECURITY4ACCOUNTANTS (2021) (arguing for increased auditor training in information security).

254. *See* Bagby, *supra* note 253, at 3.

255. *See id.* at 25.

256. *See id.* at 26–27. Two types of value are likely the major components comprising the axiomatic assertion that data is increasingly valuable. First, speculative reports of the intangible value of recent mergers or acquisitions are generally computed as IP and information equaling the excess of sale price over the fair market value of tangible assets. Second, prices paid to data brokers for particular queries or licensing uses of large data sets emerge in both the level of transactions and the industry's stock prices. *See, e.g.*, Jarib B. D. Fogaca*, A Company Accounting Goodwill and Its Flaws*, LINKEDIN (July 8, 2019), https://www.linkedin.com/pulse/company-accounting-goodwill-its-flaws-jarib-b-d-fogaca [https://perma.cc/HW6Z-4FM8]; STAFF OF S. COMM. ON COM., SCI., AND TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES (2013).

"owner."[257] However, that can occur only with strong ownership rights enhanced by strong security.[258] Nevertheless, information is fugacious. "Fugacity" in this context recognizes that (i) information transfers too easily to exert simple control, and (ii) intruders are often strongly incentivized to defeat information security and information assurance measures to access information.[259] Information fugacity requires the observation that, like most intangibles, information becomes nearly inexhaustible when inadequately controlled.[260] Similarly, "information wants to be free,"[261] making information costly to control adequately for most profitable exercises of exclusive exploitation. This is not an unusual characteristic, as many types of personal property rights require costly controls.[262]

There are arguments complicating reflexive treatment of PII as private property.[263] Some forms of information are ideal examples of public goods because they are non-rivalrous and inexhaustible; like other public goods, however, they suffer from the free-rider problem.[264] That is, non-rivalrous information can be "possessed, enjoyed or exploited" by many simultaneously.[265] Unlike unique tangibles, though, possession of inexhaustible, intangible information by one entity does not usually exhaust its value.[266] Information suffers from the free rider problem because is often difficult to deny others to enjoy the fruits of one entity's investment in information (e.g., creation, collection, archiving, security, error correction, analysis, use).[267] This problem is

257. *See, e.g.*, Steven H. Hazel, *Personal Data as Property*, 70 SYRACUSE L. REV. 1055, 1056–57 (2020).

258. *See id.* at 1055–60 (advocating for a property rights approach to privacy).

259. *See* Bagby, *supra* note 253, at 20; SIEGEL, *supra* note 35 at 64.

260. *See* Bagby, *supra* note 253, at 25.

261. *See generally* R. Polk Wagner, *Information Wants to be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995, 1019 (2003) (arguing the benefits of control in fostering coordination and enabling flexibility in arrangements are essential elements of promoting progress in a changing world).

262. *See, e.g.,* Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135, 140–41 (2004) (information cannot be property in the same sense as other tangible items because of cost constraints).

263. *See, e.g.*, *id.* at 137–39.

264. *See* Bagby, *supra* note 253, at 25. *See generally* Jason Fernando, *What Are Public Goods? Definition, How They Work, and Example,* INVESTOPEDIA (Mar. 20, 2022), https://www.investopedia.com/terms/p/public-good.asp. [https://perma.cc/3S8Z-VMWF]. Public goods are still goods; they cost money to design and make and are owned, ostensibly, mostly by governments. *Id.* Of course, some public goods are real estate and others are intangibles. Here, information is often available to all. *Id.*

265. *See* Bagby, *supra* note 253, at 25.

266. *See id.*

267. *See* FRISCHMANN ET AL., *supra* note 189, at 7 (arguing that with a data commons, framing it as a free rider problem leads to binary solutions.).

clearest for government or publicly developed information, making the data trust concept of particular interest in enabling Smart City information governance, for example.[268]

Recently, legal scholarship has begun to specifically address the useful potential of and form that data trusts might take.[269] This Article argues that there is substantial space for speculation and innovation about the design configuration of data trusts.[270] Some predictable developments are conceptual in form, such as architectural design, innovation management, and the clearance of impediments for deployment of various data trust forms.[271] The following Section discusses existing exemplars of data trust in the literature.

### *A. Data Trust Variants*

In this Section, three possible variants of data trusts are presented, compared and contrasted. The Type 1 architectural approach lays out the major components of the trusts and specifies their relationship links.[272] Second, the Type 2 public goods approach assumes that market failure will predominate.[273] Third, the Type 3 pro-privacy approach would depend on stronger privacy rights legislation to enable strong data trusts.[274]

#### 1. Type 1: Architectural Approach

First, Mozilla Fellow Anouk Ruhaak argues that a simple but necessary first step is needed.[275] Ruhaak takes an architectural approach to data sensing, acquisition, archiving, distribution, use, correction, deletion, and audit trails.[276] Second, researcher Stuart Mills makes a political economy comparison among the roles of various

---

268. *See* Matthew Halliday, *What Exactly Is a Data Trust?*, MARS (July 28, 2020), https://www.marsdd.com/news/what-exactly-is-a-data-trust/ [https://perma.cc/Y926-XFXZ].

269. Although much of the research comes out of the United Kingdom, Canada, and European Union, we are just now starting to see some data trust scholarship emerge in the United States. *See generally* Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L.J. 333 (2021) (proposing state-owned public trusts to hold residents' locational and personal data similar to common law arrangements to protect public assets).

270. *See supra* Part III.

271. *See generally supra* Part III.

272. *See infra* Section IV.A.1.

273. *See infra* Section IV.A.2.

274. *See infra* Section IV.A.3.

275. Anouk Ruhaak, *Data Trusts: Why, What and How*, MEDIUM (Nov. 11, 2019), https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34 [https://perma.cc/Q4MD-JB8C].

276. *See id.*

stakeholders who might participate in data trusts by examining three models: laissez-faire, data trusts, and data commons[277] as a useful comparative to construct a conceptual foundation.[278] However, neither discussion adequately addresses data leakage, data breaches, or the restrictions necessary to prevent unauthorized use.[279] In addition, neither tackles the complexity nor costs of implementing data trusts.[280] They make only indirect comments about the bundles of transactions necessary to operate either form of data trust, including: (i) a unitary societal public trust (one possible EU model) or (ii) a proliferation of competitive trusts (the likely US model).[281] Nevertheless, they both focus on data ownership and control, essential to any invocation of modern trust law.[282]

### 2. Type 2: Public Goods Perspective

Another data trust design assessment emerges from Wylie and McDonald's work,[283] which draws from a governance of public goods perspective.[284] There is a developing battle over expanding the historically recognized list of public goods that enables public financing and eases the justification of regulatory intervention into markets that initially appear or eventually behave ineffectively to avoid

---

277. Stuart Mills, *The Future of Data is Political*, MEDIUM: TOWARDSDATASCIENCE (Aug. 22, 2019), https://towsardsdatascience.com/the-future-of-data-is-political-37b1bfc83889 [https://perma.cc/TQF7-BTSF] (arguing that the laissez-faire model confers data ownership to data collectors using traditional transactions, data trusts are defined as legal structures granting stewardship over data by independent (trustee) entities, and data commons are no more than vaguely conceptualized as a technical data repository).

278. *See id.*

279. *See generally id.*; Ruhaak, *supra* note 275.

280. *See generally* Mills, *supra* note 277; Ruhaak, *supra* note 275.

281. *See generally* Mills, *supra* note 277; Ruhaak, *supra* note 275 (describing the operations of a data trust).

282. *See* Mills, *supra* note 277; Ruhaak, *supra* note 275; *see also* John W. Bagby, *Who Owns the Data*, PENN. STATE (Jan. 1, 2003), https://news.psu.edu/story/140724/2003/01/01/research/who-owns-data [https://perma.cc/2PDS-7QM2] (arguing that proprietary interests complicate an open data commons even in research communities where studied data and interpretive findings are generally considered by academic scholars as optimal when dedicated to the public domain).

283. Bianca Wylie & Sean Martin McDonald, *What Is a Data Trust?*, CTR. FOR INT'L GOVERNANCE INNOVATION (Oct. 9, 2018), https://www.cigionline.org/articles/what-data-trust [https://perma.cc/BJ28-CJVQ].

284. *See id.* Public goods are non-rival (under-produced by competitive markets) and are subject to free-rider induced waste given the tragedy of the commons. *See* Bagby, *supra* note 253, at 25. *See generally* Paul A. Samuelson, *The Pure Theory of Public Expenditure*, 36 REV. ECON. STAT. 387 (1954) (defining public goods as a trigger for public expenditure for collective consumption goods).

market-failure externalities.[285] If private data and other classes of information are considered public goods, then privacy regulation is easier to justify and property rights somewhat harder to deploy.[286] If PII is strongly regulated, it is less compelling to develop a property rights approach for data trusts as discussed here.[287] Infringement or misappropriation litigation is a less compelling remedy if privacy deprivations are closely regulated.[288] Indeed, some privacy advocates have long eschewed any property rights approach to PII, speculating that subject individuals might fail to protect themselves when unaware of their PII's value, either intrinsic or as used for derived data.[289]

Furthermore, building on Elinor Ostrom's eight principles for correcting the common's tragic difficulties,[290] Wylie and McDonald recognize that data market developments far outpace effective development of protective regulation.[291] Of course, the information commons is composed of non-excludable public goods, making them generally accessible.[292] The broad disclosure and ubiquitous accessibility of public goods in a data commons are antithetical to strong privacy and strong property rights in that PII.[293] The data trust res is envisioned as private information, so the commons and public goods characterization make such forms of custodianship unworkable to limit

---

285. *See generally* Garret Hardin, *Tragedy of the Commons*, 162 SCI. 1243 (1968). Information market failures are discussed *supra* in text and accompanying notes 20 and 156. Libertarian debate often denies the existence or intensity of market failures. *See* Tyler Cowen, *Market Failure*, LIBERTARIANISM (Aug. 15, 2008), https://www.libertarianism.org/topics/market-failure [https://perma.cc/FV5J-C2HX].

286. *See* Huq, *supra* note 269, at 366–67.

287. *See* Klosowski, *supra* note 4.

288. *See id*.

289. *See generally* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373, 1378–79, 1423–28 (2000); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1292–95, 1312–13 (2000) (arguing weakness of any property rights or state tort remedies approaches disrespects psychological interests and individual dignity).

290. OSTROM, *supra* note 183, at 90 (discussing Ostrom's eight principles for micro-commons self-governance: (1) clearly defined boundaries, (2) proportional equivalence between benefits and costs, (3) collective choice arrangements, (4) monitoring, (5) graduated sanctions, (6) fast and fair conflict resolution, (7) local autonomy, and (8) appropriate relations with other tiers of rule-making authority (polycentric governance)).

291. Wylie & McDonald, *supra* note 283.

292. *Compare* Molly McLure Wasko & Robin Teigland, *Public Goods or Virtual Commons? Applying Theories of Public Goods, Social Dilemmas, and Collective Action to Electronic Networks of Practice*, 6 J. INFO. TECH. THEORY & APPLICATION 25, 29 (2004) (noting public goods inhabit the commons), *with* Simon Vicary, *Public Goods and the Commons: A Common Framework*, 13 J. PUB. ECON. THEORY 47, 47 (2011) (arguing common pool resources risk depletion as in the "tragedy of the commons"). Some public goods uses may be subject to user fees.

293. *See* Huq, *supra* note 269, at 366–67.

transfer onward, as when the information is broadly disclosed, shared, or sold.[294]

### 3. Type 3: Pro-Privacy

The most exhaustive recent vision of data trusts emerges from the work of Sylvie Delacroix and Neil Lawrence.[295] Their pro-privacy protection perspective is largely grounded in data fugacity, which they call "leakage."[296] They concede that neither data property rights status nor a government regulation regime can provide adequate privacy protection.[297] Instead, they advocate a grassroots, bottom-up "empowerment," giving data subjects greater control ("voice")[298] than they presently wield with non-negotiable, take-it-or-leave-it form contracts.[299] Instead, a trust's power to negotiate collectively would strengthen the trustee's ability to satisfy its fiduciary duty to represent the beneficiaries' interests by serving as intermediary.[300] Finally, they recognize that beneficiaries may have preferences either for data use and protection or for the terms of any particular trust.[301] The Delacroix-Lawrence data trust conceptual framework appears to be the best configuration to inspire this Article.

Further difficulties in data trust design are evident when discussions of "privacy" actually reveal "struggles over personal information, personal power, and personal control."[302] Because so few people have the legal or technical knowledge or ability to protect their online data privacy, they feel disempowered by petitioning the government to increase their data control.[303] George Washington law professor Daniel Solove further confirms that even if privacy regulations provided individuals with more control over their data,

---

294. *See* Wasko & Teigland, *supra* note 292, at 29–30.

295. Delacroix & Lawrence, *supra* note 24, at 236.

296. *See id*.

297. *See id*.

298. *Id. (*empowerment here means shifting control over PI from brokers to subject individuals).

299. *Id.* at 236, 239. In click-wrap contracts, the offeree manifests assent to boilerplate, electronically presented terms in recurring low transactions-cost networked computer interactions (e.g., social media and platform access, privacy policies, arbitration and choice of law or forum, and IP rights). Click-wrap assent is derived from shrink-wrap assent validity (opening software packaging where license terms are visible through sealed transparent packaging). *See generally* JOHN W. BAGBY, E-COMMERCE LAW: ISSUES FOR BUSINESS, 352–53 (2003).

300. *See* Delacroix & Lawrence, *supra* note 24, at 236.

301. *Id.* at 241, 248, 249.

302. NEIL M. RICHARDS, WHY PRIVACY MATTERS 3 (2021).

303. *See id*.

because of the complexity involved with data protection, such laws are unlikely to be effective.[304]

Following the 2016 Cambridge Analytica hacking scandal, the public has become savvier and more careful with their PII.[305] Nevertheless, people still engage in actions contrary to their stated privacy preferences.[306] The public remains segmented into multiple tranches roughly describing their privacy preferences and expectations.[307] Automated contract negotiation could result in near infinite baskets of data use authorizations if such rich diversity were to be available in data trusts.[308]

### *B. Data Trusts as Bundles of Contracts*

For data trusts to become large and successful, they are likely to involve thousands of constituents, clients, customers, and various service providers.[309] As data trusts behave more like private firms, they should be analyzed under classic law and economics theory.[310] That is, it is useful to analyze them as "bundles of contracts" rather than as

304. *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 5 (2021) ("Managing one's privacy is a vast, complex, and never-ending project that does not scale. Privacy regulation often seeks to give people more privacy self-management, but doing so will not protect privacy effectively. Professor Solove argues instead that privacy law should focus on regulating the architecture that structures the way information is used, maintained and transferred.").

305. *See* Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening*, WIRED (Mar. 17, 2019, 7:00 am), https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ [https://perma.cc/9PUE-BMXY]; *In re* Cambridge Analytica LLC, FTC File No. 182 3107, Doc. No. 9383 (Dec. 18, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter [https://perma.cc/WVV7-X4PP] (settling charges of deceptive tactics that harvested PII from millions of Facebook users to inform voter profiling and targeting with pro-Republican candidate political messaging in 2016 US national election).

306. SUSANNE KLAUSING, THE RELATION BETWEEN ATTITUDE CERTAINTY AND THE PRIVACY PARADOX 1 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3937221 [https://perma.cc/67EM-B4P6] ("The privacy paradox—the question whether individuals act contrary to their privacy preferences (i.e., attitudes, concerns) when disclosing data—has received much attention. While the general notion has largely been refuted, contextual factors can still coax individuals into acting contrary to their privacy preferences.").

307. *See id.*

308. Lorrie Faith Cranor, *P3P: Making Privacy Policies More Useful*, 6 IEEE SEC. & PRIV. 50, 51–55 (2003) (arguing for automated, electronic, agent-based negotiation of privacy preferences using the P3P, Platform for Privacy Protections).

309. *See* ALINE BLANKERTZ, DESIGNING DATA TRUSTS 5 (2020).

310. *See generally* Ronald Coase, *The Nature of the Firm*, 4 ECONOMICA 386, 391–93 (1937).

individual entities.[311] The particular contracts bundled are nearly infinitely variable and may produce many different configurations, architectures, or competing forms of trust.[312] Traditionally, the United States has seen vigorous competition in markets for the most common form of trust—that used in estate planning and asset management for beneficiaries.[313] Generally, trusts are most desirable when trustees, who are experts in the subject matter, supply essential management and selection services for beneficiaries, whereas the latter are generally unskilled in investment management or are predicted to become extravagant spendthrifts.[314] Dozens of trust forms have developed over the millennium during which the trust device has evolved.[315] Similarly, most people are unskilled in how to protect their data and online privacy due to structural barriers, like lack of expertise or access to

311. *See generally id.*; Leon Trakman, Robert Walters & Bruno Zeller, *Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience*, 29 INFO. & COMMC'NS TECH. L. 218 (2020) (arguing for greater legal consistency and harmonization in the law governing consent for the use of personal data, in defining the nature of that consent, and in devising a regulatory framework that takes account of the cognitive capacities and behavior of data consumers).

312. *See* BLANKERTZ, *supra* note 309, at 18.

313. *See generally* Steven J. Oshins, *You, Inc.: Branding Yourself in a Competitive Estate Planning Industry,* ULTIMATE EST. PLANNER, (Sept. 1, 2016) https://ultimateestateplanner.com/wp-content/uploads/2016/09/September2016-SJOYouInc.pdf [https://perma.cc/GQ7E-PCY2]. In the United States, estate planning is an atomized and competitive services market that generally claims to provide highly differentiated, custom products in various product lines. Of course, state lines bound these markets in some instances. *But see* Alexandra M. Jones, *Old Days Are Dead and Gone: Estate Planning Must Keep Its Head Above Water with the Changing Tide of Technology*, 11 EST. PLAN. & CMTY. PROP. J. 161, 175–76, 181 (2018) (arguing that financial technology, such as robo-advisors, makes estate planning more competitive as service providers deploy expert systems to supplement their advice). *See generally* Oshins, *supra*.

314. *See, e.g.,* Evan J. Criddle, *Liberty in Loyalty: A Republican Theory of Fiduciary Law*, 95 TEX. L. REV. 993, 1026 (2017). Trustee expertise and fiduciary duties accommodate the needs of clients and beneficiaries best when the latter are in need of professional management and diminished conflicts of interest. *See, e.g.*, *id*.

315. *See, e.g.*, Lee-Ford Tritt & Ryan Scott Teschner, *Re-Imagining the Business Trust as a Sustainable Business Form,* 97 WASH. U. L. REV. 1, 48 (2019) (arguing flexibility and proliferation of business trust forms promises to enhance sustainability). The form that successful data trusts might eventually assume remains uncertain. Indeed, data trusts may choose some or more of the aspects of the many modern forms of trust that are well-known in business and estate planning, including, *inter alia*, constructive, inter-vivos, testamentary, resulting, spendthrift, living, charitable, special needs, qualified domestic, revocable, irrevocable, asset protection, tax by-pass, Totten. *See* Mollie Moric, *Types of Trusts: Different Types of Trust Funds Explained*, LEGALTEMPLATES (July 4, 2022), https://legaltemplates.net/resources/estate-planning/types-of-trusts/#two-main-types-of-trusts [https://perma.cc/CF6V-2GGU]. Variables in trusts include, *inter alia*, creation method; limitations on trustee powers; duration; termination; objectives; trustee replacement; beneficiary designation, identification, and elimination; and jurisdictional validity. *See e.g.*, N.C. GEN. STAT. §§ 36C-4-401–419.

relevant markets.[316] Data trusts show promise to assume one or more of the forms of common law trusts.

It may be useful to create a provisional ontology of data trust contracting.[317] As data trusts mature and definable aspects emerge, this classification scheme may need to expand. Nevertheless, anchoring contracts to existing information supply chains and online contracting styles provides useful insight and permits more immediate understanding.[318]

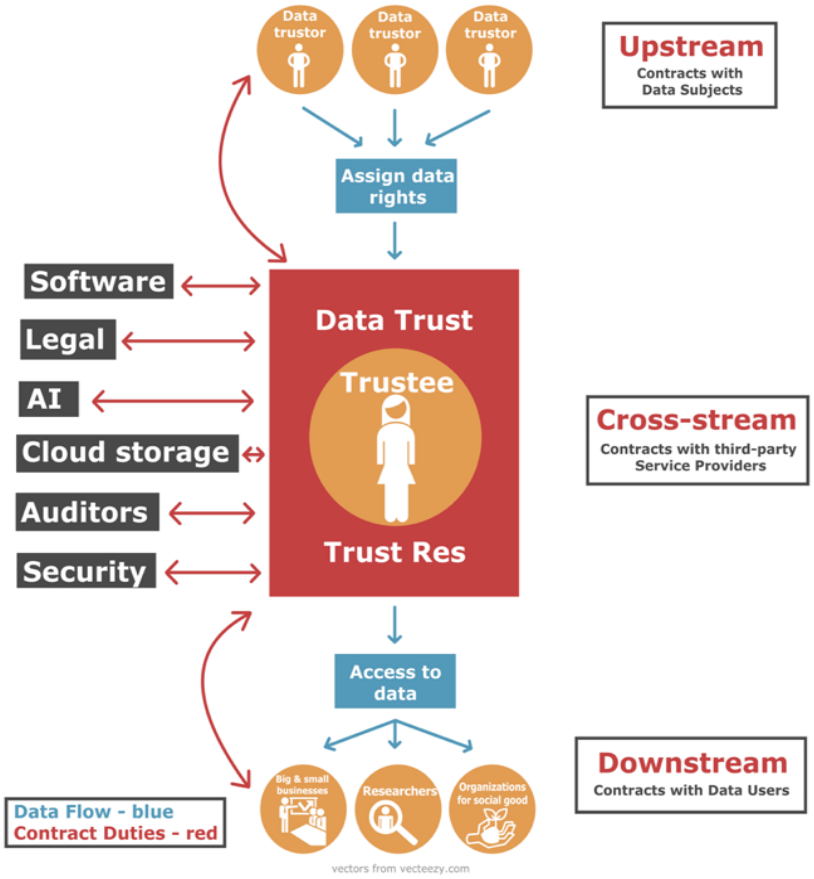



Figure 1 – Data Trust Supply Chain[319]

316. *See* Solove, *supra* note 304.

317. In philosophy and computer and information sciences, ontologies refer to systematic categorization of expected phenomena. *See generally* John F. Sowa, *Top-Level Ontological Categories,* 43 INT'L J. HUM. COMPUT. STUD. 669 (1995).

318. *See id*. at 669–70.

319. Figure 1 created by Frankie Houser. Vecteezy attribution for vectors in Figure 1: Stick Characters Posture Icon Action Figures Symbols Human Body Silhouettes 3605016 Vector Art at

1. An X-Stream Approach

As currently envisioned in the literature, data trusts are useful primarily because the trustee serves as a loyal intermediary, owing fiduciary duties to subject individuals who entrust their data to data trustees.[320] This would make it unlikely that a simple two-party model of trustor-trustee could ever emerge, and it would certainly never predominate.[321] Instead, the competitive data trusts envisioned here will likely have interactions in numerous contracts with potentially numerous parties: (i) upstream with countless trustor-beneficiaries providing data for the trust, operating as a data managing repository or platform; (ii) cross-stream with various types of service providers as necessary to enable the most effective, efficient, and competitive trust operations; and (iii) downstream with many third-party data users that seek to access the beneficiaries' data in wholesale and retail data distribution contracts.

Arguably, data trusts assume a central node function to "order match"—that is, to sell the data of trustees to satisfy specified needs of customer-users. At scale, data trusts evolve into a new form of the classic bundle of contracts. That bundle is composed of three broad types of contracts. First, there must be upstream (in the supply chain) contracts by which the trustee acquires data from trustors, settlors, or beneficiaries. Second, the trustee must contract cross-stream with service providers, which will provide service levels in the processing, distribution, and safeguarding of these data. Finally, the trustee will distribute data downstream to customers and users. This structure is similar to many traditional trusts because trustees buy, sell, and hold

Vecteezy, https://www.vecteezy.com/vector-art/3605016-stick-characters-posture-icon-action-figures-symbols-human-body-silhouettes [https://perma.cc/TQW4-6FAE]; Business Management and Human Resource Icons Set 1185186 Vector Art at Vecteezy, https://www.vecteezy.com/vector-art/1185186-business-management-and-human-resource-icons-set [https://perma.cc/D85W-AMRF]; Businessman Figure with Magnifying Glass Silhouette Style Icon 2516203 Vector Art at Vecteezy, https://www.vecteezy.com/vector-art/2516203-businessman-figure-with-magnifying-glass-silhouette-style-icon [https://perma.cc/C8GW-X2QK]; Family Mother Figure Silhouette Style Icon 2475319 Vector Art at Vecteezy, https://www.vecteezy.com/vector-art/2475319-family-mother-figure-silhouette-style-icon [https://perma.cc/7C4A-WC6J].

320. Delacroix & Lawrence, *supra* note 24, at 236.

321. *See id*. Two parties, (1) the trustor-settlor-beneficiary and (2) the trustee, would not function to distribute data to users, necessitating third parties like data customers. Furthermore, trustees would reach their work capacity with only a few clients necessitating service providers. Therefore, multiple-party data trusts are the only feasible architecture. *See id*. at 236.

assets; make discretionary judgments; and distribute assets and "returns" among various trust constituents.[322]

Upstream contracts with intermediaries, like data trustees, involve acquisition of contractual subject matter. Customary supply chains do not acquire or source their subject matter at a retail level. This is seemingly counterintuitive for most supply chains because their raw materials are generally acquired at a wholesale level. In the provision of professional services, where the client (trustor) supplies the valuable subject matter (data), the trustor's appointment of trustee serves to acquire the contract's subject matter. Data trust "entrustment" by trustor-beneficiaries is a business-to-consumer (B2C) relationship. Counterintuitively, it is also a wholesale transaction in large successful data trusts because supply chain orthodoxy views acquiring goods (e.g., services, data) as occurring at the wholesale level, even if acquired from numerous suppliers. The trustee acquires data at this wholesale level, too, but this trustee acquisition is also a retail acquisition because the trustee provides trust services—generally, a retail activity. Trustees must recruit beneficiaries because the latter are the data-producing subjects. Some automation in these transactions seems inevitable because negotiations could become too expensive to conduct in interactive, counteroffer-dominated methods of mutual assent.[323] Of course, trustee-centered contracts are not the exclusive source of trustee duties, as the fiduciary duties of loyalty and care set default responsibilities.

Cross-stream contracts between intermediaries (trustees) and their service providers are typical. Data trusts will likely require help from third-party providers because appointed trustees may not have the necessary expertise to manage all aspects of the trust.[324] Data trusts may eventually provide complex services, such as expert decision making. For example, large scale operations require advanced networks

322. *See generally* Fiduciary Matters Subcomm., ACTEC Prac. Comm., *What It Means to be a Trustee*, 31 ACTEC J. 8 (2005). Business trusts of the late nineteenth century conducted an array of anticompetitive activity that spawned the US antitrust laws. The trust form was used to skirt restrictive state corporation laws. Generally, shareholders transferred ownership in (mostly) voting shares to a trustee which influenced the separate competing, unmerged corporations as a single enterprise. Monopolistic trusts were entities that engaged in upstream, crosstream, and downstream contracts under management of a single trustee acting as fiduciary. Intangible assets (stock) were the trust res. *See* John Morley, *The Common Law Corporation: The Power of the Trust in Anglo-American Business History*, 116 COLUM. L. REV. 2145, 2163–64 (2016).

323. *See infra* text accompanying notes 395–416 (discussing click-wrap and opting).

324. *See generally* Fracassi & Magnuson, *supra* note 149, at 343–45 (arguing banks and other financial institutions have built their information technology systems to keep customer and institutional financial records as private and non-shareable as possible by hosting the data in-house or outsourcing to independent services providers with very strict confidentiality).

supplied by telecommunications service providers to interact with counterparties. Furthermore, data trusts will likely require other expertise, enabling data trusts to deliver innovative information processing, audits, and cybersecurity. In addition, oversight will likely require contracts for independent monitoring and audit. The trust document will likely require auditing of both the management of the trust as well as compliance with use limitations on the data users.

Downstream contracts between intermediaries and third-party data users for the trust's subject matter (data) should be considered retail transactions. "Sales" of the data in a data trust are likely to be in the form of a license.[325] Users of a data trust's data accumulations[326] occupy the data user function for data transfers from the trustee-intermediary. Ostensibly, these clients expect to use the data in analyses, inspiring advertising and assessment of individuals (dossiers) or group generalizations for other future contracting or "influencing." Nevertheless, this robust retail trade does not preclude wholesale downstream contracts. Licensing large data sets also seems plausible, as when the licensed data grows large enough to approach the size of big data.

Most of these purposes are typical in business-to-business (B2B) relations.[327] Nevertheless, some downstream retail B2C data

325. *See* Guinness, *supra* note 52; *supra* text accompanying note 120. Licensing generally permits sales to multiple buyers of the same data. Assignments generally require exclusive, one-time alienation of the contract subject matter to only a single buyer. Data trusts would appear to need to deploy a licensing model to become effective as a recurring intermediary. Such licenses could conceivably follow IP licensing models where the subject matter are databases or their selective content. For example, standard form data use licenses could grant data users rights to use the data in AI algorithms for limited or broad purposes, such as target advertising. Data trusts might include licensing limits on duration of each use and prohibit resale of raw data. Licenses are hugely complex, the multiple contours of which are well beyond the scope of this Article. *See, e.g.*, Michael R. Oppenheim & Roxanne Peck, *From Print to Online: The Complexity of Licensing E-Reference Resources*, *in* ENVISIONING THE FUTURE OF REFERENCE: TRENDS, REFLECTIONS, AND INNOVATIONS 111, 111–16 (2020).

326. There are a number of options for how data, or more likely access to data, can be provided. A data trust could provide data to the data user with strict use limitations, access to the set held by the trusts could be provided, such as in the case where the trust is in the form of a platform, or it is possible that eventually analytics could be performed within the trust platform itself on behalf of SMEs or nonprofit organizations who may not have the technical ability to make use of the data but have specific needs. This could constitute an AI-as-a-Service function for the trustee, creating revenue for the operation of the trust. *See, e.g.*, Hanna Klienings, *What Is AIaaS? Your Guide to AI as a Service*, LEVITY (Oct. 5, 2022), https://levity.ai/blog/aiaas-guide [https://perma.cc/ND5N-KZZS].

327. *See* Susanne Morris, *B2B Data: The Complete Guide for 2022,* CORESIGNAL, (Feb. 23, 2022), https://coresignal.com/blog/b2b-data/ [https://perma.cc/TZK5-J584]. B2B and B2C are frequently used abbreviated shorthand jargon in the analytics of internet commerce architectures. *See*, *e.g.*, MARTIN FRIES, DATA AS COUNTER-PERFORMANCE IN B2B CONTRACTS 1, 7 (2019).

transactions are arising.[328] Such downstream sales as individual dossier sales are becoming a retail trade as the public continues the current trend of purchasing background checks. However, this could only be permitted in compliance with the trust document, and at least some privacy obsessive data subjects might refuse to readily consent to this unless it becomes socially standardized or is obviously needed to engage in particular relationships.[329]

There is a clear and important distinction between the downstream data trust contracting envisioned here and current practices of data licensing by data brokers.[330] This distinction actually drives the development of data trusts as envisioned here. Data brokers decide what data is transferred to customers, determine when the transfer occurs, and do not seek permission from subject individuals.[331] By contrast, data trustees are upstream actors, contractually required to distribute data according to the trust provisions and bound by fiduciary duties.[332] By stark contrast, data brokers have no fiduciary obligations to data subjects.[333] In data brokerage practice, data subjects generally have no say in how their data is used or shared, and data subjects generally do not directly consent to any distributions of their data.[334]

Here, data brokers are relevant because they could stand in direct competition with data trusts. The emergence of data trusts, then, may incentivize data brokers to align their business models more with

---

328. For example, individuals considering dating relationships are frequently in search of dossiers that exhibit the temperament and risk profile of candidate dating partners, a retail distribution. *See* Alyson Krueger, *The Best Ways to 'Research' Someone You Meet Online*, FORBES (Apr. 30, 2014, 12:21 PM), https://www.forbes.com/sites/alysonkrueger/2014/04/30/the-best-ways-to-research-someone-you-meet-online/?sh=926c6862cde4 [https://perma.cc/LF6A-GM8F].

329. *See* Delacroix & Lawrence, *supra* note 24, at 236. Similar reticence to and broad or general distribution of personal financial data inspires the requirement of specific permission for every data distribution under Truth in Lending or for protected healthcare information under HIPAA. Other examples abound. *See* DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE (2005), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/TTJ7-KF7R].

330. *See generally* JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS (2021) (explaining the lack of regulation around the "buying, aggregating, selling, licensing, and otherwise sharing" of individuals' data by data brokers).

331. STAFF OF S. COMM. ON COM., SCI., AND TRANSP., *supra* note 256, at 3.

332. Delacroix & Lawrence, *supra* note 24, at 236.

333. *See supra* note 181 and accompanying text.

334. *See generally* SHERMAN, *supra* note 330; STAFF OF S. COMM. ON COM., SCI., AND TRANSP., *supra* note 256, at 3; ROBERT GELLMAN & PAM DIXON, DATA BROKERS AND THE FEDERAL GOVERNMENT: A NEW FRONT IN THE BATTLE FOR PRIVACY OPENS, 10–11 (2013); CARY SHENKMAN, SHARON BRADFORD FRANKLIN, GREG NOJEIM & DHANARAJ THAKUR, LEGAL LOOPHOLES AND DATA FOR DOLLARS: HOW LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE BUYING YOUR DATA FROM BROKERS 5 (2021).

this emerging model of data trusts. Data brokers are the closest existing potential competitor to data trusts, and competitive pressures could incentivize data brokers to more closely operate like data trusts.[335] The following Section further analogizes data trustee contracts to other intermediated markets because existing relationships provide good starting points for further design experimentation.

### 2. Three Predicted Bundles of Data Trust Contracts

First, this Section expresses a vision of data trusts that provides individual beneficiaries with the contractual flexibility to ensure access to their data stores on terms favorable to beneficiaries.[336] Intermediation—the role of go-between, matching customer orders with supplier information—will eventually endow successful data trusts with market power.[337] This will leverage the large databases aggregated from numerous data trust beneficiaries.[338] Large databases will constitute a form of critical mass,[339] particularly for larger data trusts, as more complete data collections become more valuable.[340] The larger the data trust, the more bargaining power its beneficiaries may have to leverage their PII to secure better deals with data users.[341]

However, when beneficiaries switch between different data trusts, trustees may have to bear switching costs.[342] For example, trust switching might force trustees to retrieve data under licenses already sold, terminate usage rights over data previously transferred onward, and indemnify whatever liability might arise therefrom.[343] In such

335. *See* STAFF OF S. COMM. ON COM., SCI., AND TRANSP., *supra* note 256, at 3.

336. Delacroix & Lawrence, *supra* note 24, at 252.

337. *See* OECD, THE EVOLVING CONCEPT OF MARKET POWER IN THE DIGITAL ECONOMY 24 (2022), www.oecd.org/daf/competition/the-evolving-concept-ofmarket-power-in-the-digital-economy-2022.pdf [https://perma.cc/6BGQ-D94T].

338. *See id.*

339. Critical mass is a key attribute of network industries representing the minimal size asset base to command market power. *See generally* CARL SHAPIRO & HAL VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1998). Network effects accumulate as enhanced network value with the achievement of critical mass and the addition of many nodes and links in the network. *See id.* For example, two fax machines using the same communication standard are worth much less than millions of fax machines using a single inter-operable communications protocol. *See id.*

340. *See* John Morrell, *Does More Data Equal Better Analytics?*, DATAMEER BLOG (July 1, 2021), https://www.datameer.com/blog/does-more-data-equal-better-analytics/ [https://perma.cc/SU29-CUB7].

341. *See id.*

342. *See* Delacroix & Lawrence, *supra* note 24, at 243.

343. Unless downstream contracts prohibit license revocation, the default is that licenses can be terminated by either party. This would necessitate destruction, erasure, or other cessation

situations, termination fees for beneficiaries could be justified and would constitute a form of lock-in.[344] Lock-in reinforces the trustee's market power as an intermediary in negotiations with large-scale, downstream data customers.[345] Lock-in is often a prerequisite to the achievement of network effects.[346] However, if the contracting parties bind themselves to lock-in terms or switching fees up front, it would be considerably more difficult for one party to surprise the other with a revision later on.[347] Of course, trustees maintain more robust flexibility and avoid switching costs with the contractual ability to change terms of service at will.[348]

Second, an optimistic vision for data trusts would result in a somewhat different bundle of contracts. Some data trusts may gain success if they provide multiple services.[349] Under a "one-stop shopping" model featuring replete in-house expertise, data trusts could grow large enough to accumulate a wide variety of expertise and function wholly in-house. In-house expertise and functionality could obviate at least some cross-stream service providers. For example, banks have often "housed" banking transactions, customer relationship management,

---

of downstream use of data withdrawn from a data trust or later limited by the beneficiary's wish, will, or desire. *See generally* C. Surya, S. Banumathi, A. Neelavathi, B. Pooja & R. Manonmani, *Securing Data and Providing Privacy Assurance using Revocation in Distributed Cloud Server,* 8 INT'L. J. COMPUT. TECHNIQUES 280, 281 (2021) (arguing for feasibility of functional revocation in cloud storage arrangements appropriate when security is compromised); Sidley Austin, LLP, *The Terms "Revocable" and "Irrevocable" in License Agreements: Tips and Pitfalls*, CASETEXT (Feb. 21, 2013), https://casetext.com/analysis/the-terms-revocable-and-irrevocable-in-license-agreements-tips-and-pitfalls [https://perma.cc/LM9N-333N].

344. *See* Jan Krämer, *Personal Data Portability in The Platform Economy: Economic Implications and Policy Recommendations,* 17 J. COMPETITION L. & ECON. 263, 264, 272 (2020) (arguing that the GDPR gives EU consumers rights to port their personal data between digital service providers).

345. *See generally* JOSEPH FARRELL & PAUL KLEMPERER, *Coordination and Lock-In: Competition with Switching Costs and Network Effects*, *in* 3 HANDBOOK OF INDUSTRIAL ORGANIZATION 1967 (2007). For example, cell providers have traditionally used several methods to lock in customers, including hardware (SIM card) and contractual methods (termination fees, minimum service contracts). *See* Jeremy Laukkonen, *What Is a Vendor Lock-In?*, SMARTCAPITALMIND (Oct. 28, 2022), https://www.smartcapitalmind.com/what-is-a-vendor-lock-in.htm [https://perma.cc/S7RB-A9LS] Some lock-in schemes have been banned (landline and cellular full mobile number portability). *See generally* 47 U.S.C. § 251(b)(2).

346. *See generally* SHAPIRO & VARIAN, *supra* note 339.

347. *See generally* FARRELL & KLEMPERER, *supra* note 345.

348. *See* Delacroix & Lawrence, *supra* note 24, at 249 (changing terms of service at the service provider's whim and without separate user (here, data supplier) assent has become the predominate model).

349. *See generally* Nicholas Pasquarosa, *Here's How You Can Expand Your Service Offerings to Grow Company Revenue*, FORBES (July 31, 2019, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2019/07/31/heres-how-you-can-expand-your-service-offerings-to-grow-company-revenue/?sh=7d3042631a48 [https://perma.cc/2DGR-CCHC].

asset custody (safe deposits and vaults), and investment management—basically all their essential services—under one roof, owned or controlled by the bank entity and its affiliates or subsidiaries.[350] However, another model could provide such services by outsourcing these internal functions; such practices have grown significantly since World War II.[351] The outsourcing trend works to limit slack internal capacity by trimming payrolls and by more effectively acquiring cutting-edge expertise externally from specialized vendors, outside service providers that have their own strong reputations.[352] Offshore outsourcing, particularly of the information technology needed for data trust operations, further complicates[353] the cross-stream, essential service provider component of data trusts' bundles of contracts. Outsourcing outside the data trustee firm's jurisdiction risks increased managerial uncertainties and cultural, language, and legal and regulatory disparities such as contract enforcement, litigation expenses, and IP infringement.[354] For example, it is hard to imagine data trust operations without the cross-stream outsourcing of cloud services and telecommunications. Rights vindication is complicated by offshoring to cloud service providers residing in other nations.[355]

Third, data trusts, according to the beneficiaries' preferences, may enable the selective distribution of data downstream. This is another possible bundle of contracts that is generally envisioned, one in which data trusts will be designed to enable more highly selective distribution of data downstream in accordance with beneficiaries'

---

350. *See, e.g.*, Jonathan R. Macey, *The Business of Banking: Before and After Gramm-Leach-Bliley*, 25 J. CORP. L. 691, 719, 721–22 (1999) (arguing Congressional intent of Gramm-Leach-Bliley and its privacy provisions was to repeal the Glass-Steagall walls separating financial services to make US banks more competitive with European and Asian "universal banks").

351. *See* ANDREA GONZALES, DAVID DORWIN, DIWAKER GUPTA, KIRAN KALYAN, & STUART SCHIMLER, OUTSOURCING: PAST, PRESENT AND FUTURE 3.

352. *See, e.g.*, Victor-Adrian Troacă & Dumitru-Alexandru Bodislav, *Outsourcing. The Concept*, 19 THEORETICAL & APPL'D ECON. 51, 51, 55–56 (2012), http://store.ectap.ro/articole/734.pdf [https://perma.cc/9WCF-NMV4] (analyzing outsourcing evolution as a response to rising wages and other production costs).

353. *See generally* John W. Bagby & Joseph J. Schwerha, *International Aspects of Migrating Digital Forensics in the Cloud*, 10 DIGIT. EVIDENCE ELECT. SIGNATURE L. REV. 81, 84 (2013) (discussing jurisdictional challenges of regulation or litigation over data residing on impermanent cloud repositories given the competitive cloud computing environment, which is conducive to near effortless transfer of that data among cloud service vendors and likely to frequently cross national borders to reside in different domiciles of alternate cloud servers).

354. *See, e.g.*, DAMIAN MURBERG, IT OFFSHORE OUTSOURCING: BEST PRACTICES FOR US-BASED COMPANIES 3, 41 (2019) (offshoring essential services presents a conundrum when outsourcing decisions are driven primarily by cost-savings pressures).

355. *See* Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 315–16 (2013).

individual preferences. Data trustees could conceivably use human expertise, or perhaps expertise recommended by AI systems,[356] in accordance with the trust document to determine what is "best" for all beneficiaries or for a select group of beneficiaries. Subject individuals with strong privacy rights orientation might agree for only limited data distribution to data users. However, data trust beneficiaries with lesser expectations for their privacy protection might consent to broader data distribution among numerous downstream data users.

Based on the foregoing, data trusts will operate as classic bundles of contracts in all three data trust contracting situations: (i) upstream data acquisition from trustor-beneficiaries, (ii) in-house processing or cross-stream acquisition of essential professional services, and (iii) downstream in sales of data licenses in the distribution to various data users.[357]

### 3. Take Care in "Crossing the Streams"

As data trusts grow and achieve widespread notoriety, their reputations will be correspondingly enhanced. Unfortunately, their intangible asset of goodwill is vaguely defined and subject to inconsistent standards of evaluation.[358] Aside from the typical factors influencing goodwill (e.g., competitive prowess, which generally manifests in ratings; satisfied customer testimonials, often of trustors, beneficiaries, and data suppliers; expert assessment and advertising), intermediaries shine when successfully vindicating client rights.[359] Consider how law firms and tax services regularly tout their winning track records.[360] Investment trusts tout their return on investment.[361]

---

356. *See* Klienings, *supra* note 326. In this application of AI, the expertise in satisfying beneficiary preferences could be devised using machine learning, in much the way recommendations systems, based on AI, customize various social media experiences. *See id*.

357. *See supra* Section III.B.

358. *See* Fogaca, *supra* note 256.

359. *See id*.

360. *See, e.g.*, *Top Verdicts & Settlements*, THOMAS J. HENRY L., https://thomasjhenrylaw.com/campaigns/nationwide-injury-attorneys-lp/?utm_source=google&utm_medium=cpc&gclid=Cj0KCQjwkt6aBhDKARIsAAyeLJ3cHKXQoG5rrU_DsnuC3JYk_DMYZC5o08yF52Padyh_uMWIOOe6oUwaAmFeEALw_wcB [https://perma.cc/9UEU-RQXL] (last visited Nov. 6, 2022); *Firm Overview*, MARCUM LLP, https://www.marcumllp.com/firm [https://perma.cc/D4X5-RBAN] (last visited Nov. 6, 2022).

361. *Are Commercial Mortgages Already in Your Investment Portfolio?*, AVATAR FIN. GRP., https://info.avatarfinancial.com/commercial-mortgage-investment-opportunity?utm_term=commercial%20property%20reit&utm_campaign=Landing+Page+REIT+(Search)&utm_source=adwords&utm_medium=ppc&hsa_acc=4162510847&hsa_cam=15844130314&hsa_grp=130848471806&hsa_ad=573800725179&hsa_src=g&hsa_tgt=kwd-

How might such mechanisms enhance the competitive claims of data trust service reliability? This problem is likely to remain elusive.

The problem is even more acute for the range of hypothetical data trusts envisioned in other current literature because their enforcement of downstream data usage, vindication of data transferred onward,[362] and recall of data in certain situations could be costly.[363] In addition, cross-stream breach of contract enforcement against service providers also may involve cross-border enforcement, as it does in some other service industries.[364] Therefore, the reputation of data trusts depends on mastering enforcement at precisely the time that both the beneficiary and trustee may be ignorant of the data's misuse. Contrasted with other trust rights vindications where asset losses are more readily evident, data trusts may suffer major challenges to privacy rights vindication.[365] Both data subjects and trustees too often will have imperfect knowledge of any data leakage or data inaccuracy until some outsider uses that data negatively against the data subject.[366]

To efficiently resolve the disputes that will inevitably arise, internal dispute resolution procedures or access to reliable and efficiently operated dispute resolution mechanisms will be needed. Online dispute resolution (ODR) might enable data trusts to vindicate

---

451411739976&hsa_kw=commercial%20property%20reit&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjwkt6aBhDKARIsAAyeLJ048gqQk_h3-AB99MwfYp0RaRlDdUAX-AlOobx1gh4pHYUtXO_A9_4aAgViEALw_wcB [https://perma.cc/ZV9U-5HWV] (last visited Nov. 6, 2022).

362. *See* Christopher Kuner, *Onward Transfers of Personal Data Under the U.S. Safe Harbor Framework*, PRIV. & SEC. L.R., 2009, at 2 (describing "onward transfer" as the disclosure of data by any custodian in the information supply chain).

363. *See supra* notes 261–62 and accompanying text.

364. Domestic content regulation of manufacturing might be adapted to require domestic provision of some or all cross-stream services to minimize data leakage and better enable litigation success in vindicating the rights of beneficiaries in their home domiciles. *See* CORWELL MORING, THE ABCS OF CROSS-BORDER LITIGATION IN THE UNITED STATES (2008), https://www.crowell.com/files/ABC-Guide-to-Cross-Border-Litigation_Crowell-Moring.pdf [https://perma.cc/768Y-ZFHL]. While international arbitration is a common B2B dispute resolution alternative, it seems highly unlikely to satisfy the needs of data trust trustor-beneficiaries. *See* AAA-ICDR, ARBITRATION REMAINS A TRUSTED VENUE FOR RESOLVING B2B DISPUTES (Feb. 27, 2018), https://www.adr.org/sites/default/files/document_repository/180223_AAA_ICDR_Arbitration_Caseload_Data_Press_Release.pdf [https://perma.cc/VU6J-E7HP].

365. *See Trust Beneficiary Rights | Can a Beneficiary Sue a Trustee?*, KEYSTONE L. GRP., (Oct. 21, 2022), https://keystone-law.com/rights-of-a-trust-beneficiary-to-sue-a-trustee/ [https://perma.cc/73U5-29MD].

366. *See, e.g.*, Joanna Redden, Jessica Brand & Vanesa Terzieva, *Data Harm Record*, DATA JUST. LAB (Aug. 2020), https://datajusticelab.org/data-harm-record/ [https://perma.cc/37JU-U26H] (describing harms such as targeting the vulnerable, data breaches, and political manipulations).

the interests of upstream beneficiaries.[367] However, much of the ODR experience in the United States has been developed as the result of court-annexed alternative dispute resolution (ADR) and as required in widespread terms of service (ToS) in online shopping, the latter providing greater ODR access to consumer claimants.[368] Mandatory arbitration clauses require submission of disputes to external forms of ADR, a fairly effective method deployed by the securities industry in retail brokerage contracts as well as in B2B supply chain relations.[369]

This situation, where ODR enables a client to vindicate individual rights in personal data, appears to be novel to data trust rights vindication.[370] However, challenges to ODR's success will arise, given that data trust litigation—up-, cross-, and downstream—will often span jurisdictional borders. Increasingly, ADR, and generally ODR, involve virtual tribunals where participants, parties, and decision-makers attend remotely in live participative environments.[371] Automated tribunals or other automated dispute resolution could develop, too, but are likely to require some additional development,

---

367. *See, e.g.*, A.B.A. CTR. FOR INNOVATION, ONLINE DISPUTE RESOLUTION IN THE UNITED STATES 1 (Sept. 2020); Erika Rickard & Qudsiya Naqui, *How Well Does Online Dispute Resolution Help Resolve Lawsuits Outside the Courtroom?* PEW CHARITABLE TR. (Jan. 19, 2021), https://www.pewtrusts.org/en/research-and-analysis/articles/2021/01/19/how-well-does-online-dispute-resolution-help-resolve-lawsuits-outside-the-courtroom [https://perma.cc/8EKB-8EK4].

368. *See generally, e.g.*, Arakelian Minas, Olga Ivanchenko & Oleg Todoshchak, *Alternative Dispute Resolution Procedures Using Information Technologies: Legal Regulation in the European Union and the USA*, 9 AMAZONIA INVESTIGA 60 (2020) (reporting large ODR deployments by Amazon and eBay).

369. *See* GARY SHORTER, CONG. RSCH. SERV., IF12076, LEGISLATION TO REPEAL MANDATORY SECURITIES ARBITRATION (2022). ADR is widely used in labor, employment, and financial services disputes. *See, e.g.*, May Olivia Silverstein, *Introduction to International Mediation and Arbitration: Resolving Labor Disputes in the United States and the European Union*, 1 AM. U. LABOR & EMP. L.F. 101, 108–09 (2011); *Dispute Resolution Statistics*, FINRA, https://www.finra.org/arbitration-mediation/dispute-resolution-statistics [https://perma.cc/R2Y8-VHFR] (last visited Nov. 6, 2022).

370. *See* Minas et al., *supra* note 368. Classic configuration of ODR, like much ADR, in rights vindication is pursued by parties although there is an increasing use of representatives, both lawyers and non-lawyer advocates. Classic arbitration clauses have sought simplicity and cost reduction by barring representation and ADR representation by non-lawyers has been hotly contested. *See generally* David W. Rivkin, *Keeping Lawyers Out of International Arbitrations*, 9 INT'L FIN. L. REV. 11, 11–12 (1990).

371. *See* JEAN-PIERRE DOUGLAS-HENRY, RICHARD F. HANS, JEFFREY ROTENBERG, JONATHON ELLIS, CHARLES ALLIN & GAJENDRAN BALACHANDRAN, VIRTUAL HEARINGS 2021 (Sept. 2021), https://www.dlapiper.com/~/media/files/insights/publications/2021/07/virtual-hearings_booklet.pdf [https://perma.cc/95FM-DDTK].

testing, and verification before becoming sufficiently ubiquitous for data trustee reliance.[372]

Much of the litigation over privacy rights, enforceability of trusts, and breaches of contract are matters of state law.[373] Conflicts of laws complexities seem predictable. Data trust rights vindication must rely on doctrines of full faith and credit, collateral estoppel, res judicata, and comity.[374] To make data trust litigation decisions enforceable in other jurisdictions, the data trust form of organization may require recognition under international treaties.[375] Indeed, additional treaties may become necessary to fully enable data trusts.[376]

In the United States, the creation and strengthening of privacy rights are generally within state police powers, particularly when privacy is conceived as protecting property rights in PII, avoiding intrusions from societal predators, or preventing contacts that endanger health, safety, welfare, or morals.[377] Data trusts simplify the process by which a data subject may vindicate her rights.[378] However, they will arguably exacerbate existing jurisdiction challenges in privacy

372. *See generally* Mariusz Załucki, *AI and Dispute Resolution*, *in* EL DERECHO PÚBLICO Y PRIVADO ANTE LAS NUEVAS TECNOLOGÍAS 338 (J. Garcia Gonzalez, A. Alzina Lozano & G. Martin Rodriguez eds., 2020), http://dx.doi.org/10.2139/ssrn.3636187 [https://perma.cc/9ZMA-N6T4] (describing some examples of automated dispute resolution); Jeremy Barnett & Philip Treleaven, *Algorithmic Dispute Resolution—The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies*, 61 COMPUT. J. 399, 399, 407 (2018) (discussing the future of algorithmic dispute resolution).

373. *See* U.S. CONST. amend. X. Clearly, some privacy claims fall under federal jurisdiction, primarily as (1) complaint-triggered enforcement actions as unfair or deceptive trade practices by the Federal Trade Commission under FTC Act § 5, 15 U.S.C. § 45, (2) financial privacy violations at various types of financial institutions under Gramm-Leach-Bliley, 15 U.S.C. §§ 6801–09 and regulations promulgated thereunder, or (3) in the healthcare realm under HIPAA privacy and security standards, *e.g.*, 42 C.F.R. § 403.812. Nevertheless, most privacy and data security laws are state laws. State common law covers torts, contracts, and trust invoking state courts, unless diversity jurisdiction applies. *See, e.g.*, Erie R.R. Co. v. Tompkins, 304 U.S. 64 (1938).

374. Rex R. Perschbacher, *Rethinking Colatteral Estoppel: Limiting the Preclusive Effect of Administrative Determinations of Judicial Proceedings*, 35 FLA. L. REV. 422, 466 (1983).

375. Benjamin Greze, *The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives*, 9 INT'L. DATA PRIV. L. 109, 110–11 (2019).

376. *Compare id.*, *with* EXTRATERRITORIAL ENFORCEMENT: DEVELOPING NORMS FOR THE INFORMATION SOCIETY (2018), https://law.yale.edu/sites/default/files/area/center/isp/documents/extraterritorial_enforcement_paper.pdf [https://perma.cc/XND6-CK56].

377. *See generally* U.S. CONST. amend. X.; Jacobson v. Mass., 197 U.S. 11 (1905) (holding a mandatory vaccination program was valid exercise of state police power).

378. *See generally* JESSICA FJELD, NELE ACHTEN, HANNAH HILLIGOSS, ADAM NAGY & MADHULIKA SRIKUMAR, PRINCIPLES ARTIFICIAL INTELLIGENCE: MAPPING CONSENSUS IN ETHICAL AND RIGHTS-BASED APPROACHES TO PRINCIPLES FOR AI, 23, 33 (2020).

litigation.[379] Complications escalate when data use extends beyond state or national borders.[380] As more nations consider this data trust alternative to protect privacy rights, data subjects may seek out data trusts that provide protection across international borders to better enable a global, uniform data trust structure.[381] A uniform data trust structure might enable international data flows. As with most modern, novel business models, designs that provide data protection sufficient to meet the laws in the loci of the various data subjects have more promise for success.[382]

### *C. Enabling Data Trust Contracting*

Data trusts arguably will follow and adopt many of the developing electronic contracting practices.[383] Data trust contracts could be informal,[384] bilateral, or multilateral agreements,[385] memorialized by traditional, "wet-signed" writings or electronically executed writings resulting from mutual assent. Some of these agreements will likely be concluded after negotiations using traditional offers, counteroffers, and acceptances. Absent special legislation, data

379. *See, e.g.*, Kate Westmoreland, *Jurisdiction Over User Data—What Is the Ideal Solution to a Very Real World Problem?*, CTR. FOR INTERNET & SOC'Y (July 24, 2014, 6:11 PM), http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problem [https://perma.cc/HDC4-98YL].

380. *See, e.g.*, *id.*; Margaret Byrne Sedgewick, *Transborder Data Privacy as Trade*, 105 CALIF. L. REV. 1513, 1528 (2017).

381. *See generally* Javier Lopez-Gonzalez, *How Privacy Pros Can Help the OECD's Cross-Border Efforts,* IAPP (May 24, 2022), https://iapp.org/news/a/how-privacy-pros-can-help-the-oecds-cross-border-efforts/ [https://perma.cc/LUM9-ZNX2].

382. *See generally* ERIC LACHAUD, ISO/IEC 27701: THREATS AND OPPORTUNITIES FOR GDPR CERTIFICATION (2020), https://ssrn.com/abstract=3521250 [https://perma.cc/NG7A-QPFV] (arguing for extraterritoriality of ISO standards). As Toulouse Business School Professor W. Gregory Voss explains, although there is a potential for the harmonization of *practices*, it is unlikely that there will be a harmonization of *privacy law* to facilitate cross-border data flow. W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 457 (2019).

383. *See supra* notes 308, 324 and accompanying text.

384. Informal in the sense that law does not require particular forms, as extant in negotiable instrument law, for enforceability. *See* David M. Steingold, *The UCC and Negotiable Instruments – Part 1 of 2*, NOLO, https://www.nolo.com/legal-encyclopedia/the-ucc-negotiable-instruments-part-1-2.html [https://perma.cc/HHP2-VM6E] (last visited Nov. 6, 2022). With uniform enabling legislation, upstream data trust contracts could conceivably constitute formal contracts. However, cross-stream and downstream data trust contracts are much less likely to be required to be in a particular form by statute.

385. Some of the idealistic visions of data trusts might envision multilateral contracts, assented to near simultaneously, upstream among trustor-beneficiaries and trustees, cross-stream between trustee and various service providers, and downstream to data customers.

trust documents would be interpreted under the common law.[386] Data trust contracts generally cover subject matter that would be classified as a supply of information in a commercial contract context, therefore classified as contracts for services, not goods under the Uniform Commercial Code.[387]

Data trusts, as bundles of many contracts, are likely to have data trustee operators who prefer the cost savings of electronic contracting if it is available and cost-effective. Automated electronic contracting (eContracting) is still nearly impossible without fixed terms and conditions in take-it-or-leave-it situations.[388] This explains the predominance of standardized ToS. Complex negotiations require consideration of dozens of trade-offs generally impossible with automated contracting.[389] This turns fully automated eContracting into a design quest for low-cost implementation of complex contracts.[390] The current risk is that, even after the data trust form is negotiated, future beneficiaries will be unable to efficiently renegotiate because they are confronted with a take-it-or-leave-it form to gain entry.[391] Therefore, it is difficult to predict successful, large-scale, economically efficient data trust operations without deploying at least two forms of electronic contracts. First, both the B2C upstream recruitment of data subjects and the B2C downstream retail distribution of data to the data users will likely necessitate the simplicity of click-wrap assent.[392] Second, data trusts' contracting in B2B relations, both in cross-stream outsourcing with service providers and in data license sales to large

386. *See* Porcaro, *supra* note 228, at 332, 344.

387. *See* Richard K. Lomotey, Sandra Kumi & Ralph Deters, *Data Trusts as a Service: Providing a platform for multi-party data sharing*, 2 INT'L J. INFO. MGMT. DATA INSIGHT, Apr. 2022, at 1–2, 4, 7; *see also What Is the UCC (And What Doesn't It Cover)?*, INDEED, https://www.indeed.com/hire/c/info/what-is-the-ucc [https://perma.cc/9EYE-4RVW] (last visited Nov. 19, 2022).

388. *See, e.g.*, Christopher D. Clack, *Smart Contract Templates: Legal Semantics and Code Validation*, 2 J. DIGIT. BANK. 338, 342, 346 (2018).

389. *See* Stephan Sonnenberg & James L. Cavallaro, *Name, Shame, and Then Build Consensus? Bringing Conflict Resolution Skills to Human Rights*, 39 WASH. U. L.J. & POL'Y 257, 286 (2012); *What Are Smart Contracts on Blockchain?*, IBM, https://www.ibm.com/topics/smart-contracts [https://perma.cc/668S-42JY] (last visited Nov. 6, 2022).

390. *See generally* Kristen Lamb, *Blockchain and Smart Contracts: What the AEC Sector Needs to Know* (Ctr. for Digit. Built Britain, Working Paper No. CDBB_REP_003, 2018) (exemplifying blockchain's use in the finance sector as a low-cost contracting method with the potential to automate complex processes).

391. *See, e.g.*, Eric Goldman, *The Crisis of Online Contracts (As Told in 10 Memes)*, NOTRE DAME J. EMERGING TECH. BLOG (Aug. 30, 2021), https://ndlsjet.com/the-crisis-of-online-contracts-as-told-in-10-memes/ [https://perma.cc/MK5C-WFPX] (arguing significant empirical research denies consumers intend binding obligation when clicking through most boilerplate online agreements).

392. See *supra* note 299 and accompanying text.

downstream customers, may eventually involve automated negotiations and automated mutual assent.[393]

### 1. Click-Through Assent and Opting: In vs. Out

Two types of counterparties interacting with US-style competitive data trusts seem likely to manifest mutual assent using click-through methods.[394] First, after data trusts become commonplace, data trust beneficiaries seem likely to be able to identify a promising data trust vendor through an online search.[395] It might be expected that beneficiaries will identify data trust ToS as closest to their needs when counterparties "pair up" using various channels of advertising, as through online search and independent recommendation services.[396] The data trust beneficiary would then achieve a "conclusion of the agreement" (accepting the offer, agreeing, and likely executing a writing) using click-wrap or click-through assent.[397] This probably will constitute an opt-in to the privacy policies disclosed or promised by the data trustee's ToS.[398]

---

393. *See infra* Section IV.C.2.

394. *See, e.g.*, Specht v. Netscape Commc'ns Corp., 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d. Cir. 2002).

395. Of course, it is expected that many will wonder what types of entities will "step up to the plate" to enter the data trustee business. There is also predictable conjecture on particular data trust business practices. This Article has proposed that data trustees might emerge from traditional professional consultants (i.e., lawyers, accountants, brokers, investment advisors) or enter the market de novo from the ranks of other third-party service providers, such as telecommunications, cloud service providers, or the data processing industry. Data trust recruitment of trustor-beneficiaries might also assume the forms of supplemental consulting, or a form of financial services delivered by attorneys, accountants, financial services retail vendors, and broker-dealers. With such direct customer-facing models, both electronic contracts and written contracts requiring "wet signatures" suit existing practice or would appear plausible.

396. *See generally* Vicki Woschnick, *The 15 Most Effective B2B and B2C Marketing Strategies*, WEIDERT GRP. (Aug. 18, 2022), https://www.weidert.com/blog/most-effective-marketing-strategies [https://perma.cc/72LG-DJGT].

397. *See generally* Francis M. Buono & Jonathan A. Friedman, *Maximizing the Enforceability of Click-wrap Agreements*, 4 J. TECH L. & POL'Y, no. 3, 1999.

398. *See generally* Charles E. MacLean, *It Depends: Recasting Internet Clickwrap, Browsewrap, "I Agree," and Click-Through Privacy Clauses as Waivers of Adhesion*, 65 CLEV. ST. L. REV. 43 (2017). Most of the United States' privacy laws require deployment of some subset of Fair Information Practice Principles, standards for fair privacy relationships. Notice and consent in traditional commerce can be made expressly in written contracts or inferred from conversations or conduct. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/TNP5-R596] (discussing fair information practices); *Implied Consent*, LII, https://www.law.cornell.edu/wex/implied_consent [https://perma.cc/AJR4-FR7A] (last visited Nov. 6, 2022).

However, opt-out is the default under US privacy law, consistent with laissez-faire and sectoral privacy preference.[399] Choice among competitive data trust alternatives strongly suggests recruitment into the "winning" trust through advertising attraction, recommendation, or fiat.[400] After the choice is made, online contracting achieves the trustor-beneficiary's acceptance of the chosen data trust's privacy regime.[401] In most lower-stakes transactions—that is, in markets attracting large numbers of individual data trust trustor-beneficiaries—only one method of mutual assent manifestation seems practical: online access to notice of privacy policies; online registration, including revelation of possibly significant PII; online authorization of the data trustee; and click-through consent.[402] This would require easy-to-understand terms and not the typical 100-page notice provided by Big Tech.[403]

Under this formulation, an opt-in method may eventually grow to predominance in the United States, closely mirroring the default structure in the European Union.[404] This trend may not take over traditional data brokers but will likely become the standard among competitive data trusts[405] Arguably, if data trusts usher in any large-scale adoption of US opt-in it would counter much of the adhesion contract and user confusion literature on opt-out contracting that has emerged over the past two or more decades.[406] Privacy consent systems have generally been a binary, accept-versus-reject choice.[407] Opt-in systems would require beneficiaries to *grant* authorization for collection

399. *See, e.g.*, MacLean, *supra* note 398, at 54 n.50, 59.

400. *See generally* Eugene K. Kim, *Data as Labor: Retrofitting Labor Law for the Platform Economy*, 23 MINN. J.L. SCI. & TECH. 131 (2022) (exemplifying how a tech service provider (Google) attracts its users, which enables it to collect user data).

401. *See infra* Section IV.C.2.

402. *See* Dinesh Kumar, Amita Verma, Namita Bhardwaj & Rajinder Kaur, *Efficacy of Cloud Contracts*, 2424 AIP CONF. PROC. 030001, at 6 (2022).

403. *See* Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA HIGH TECH. L.J. 483, 496, 524 (2015).

404. Julia Palermo, *You Say Tomato, I Say Tomahto: Getting past the Opt-in v. Opt-out Consent Debate between the European Union and United States*, 9 GEO. MASON J. INT'L COM. L. 121, 123 (2017).

405. *See generally* Viljoen, *supra* note 67, at 644–48 (listing several reasons why an opt-in method may be more attractive to data subjects).

406. *See generally* Alan McQuinn, *The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules*, INFO. TECH. & INNOVATION FOUND. (Oct. 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules [https://perma.cc/J5XB-ET8A] (arguing privacy policy notice and assent in website ToS are opaque, largely ignored, and cause unpleasant surprise, all the hallmarks of adhesion contracts).

407. Ziqian Chen, Fei Sun, Yifan Tang, Haokun Chen, Jinyang Gao & Bolin Ding, *Proactively Control Privacy in Recommender Systems*, 37 ACM TRANSACTIONS ON INFO. SYS., no. 4, Art. 111, Aug. 2008, at 1, 1–2.

and use of their data.[408] Opt-out systems require subject individuals to affect an affirmative act to *deny* authorization for the collection and use of PII.[409] Businesses and data brokers in the United States generally favor opt-out, presumably because it more quickly aggregates to expand the size of their PII database and, therefore, its value.[410] US systems default to a permissive authorization for PII collection and use.[411] Such rights terminate only after beneficiaries affirmatively opt out.[412] Opt-out maximizes the data collected by automating data collection, which is why it is used by Big Tech.[413] Although data subjects would opt in to a data trust, individual users would have the ability to withdraw from a particular data trust and choose another.[414]

It seems unlikely that the whole opt-out regime in the United States will abruptly cease.[415] Two opt-out situations seem likely to persist. First, data collectors will continue to use opt-out if they do not enter the data trust business, as they may perceive no need to match data trust grant of special rights to subject individuals. Second, data trusts could conceivably offer whatever form of opting, opt-in or opt-out, as ancillary services to their upstream trustor-beneficiary clients. Under this scenario, data trusts might manage client privacy

408. *See* McQuinn, *supra* note 406.

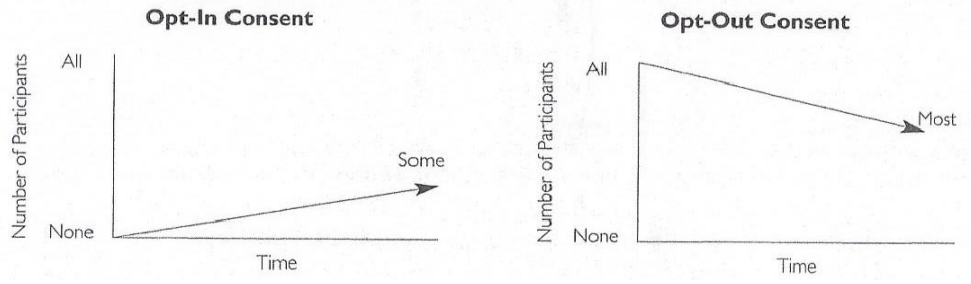
409. *Id.*

410. *See* Lauren Kaufman, *To Opt-In or Opt-Out?*, MEDIUM (Mar. 6, 2020), https://lolokaufman.medium.com/to-opt-in-or-opt-out-5f14a10bae24 [https://perma.cc/GHJ7-CPEA]

411. *See id.*

412. Any decline in size of database content advances slowly when opting-out is difficult to effect, opting is engineered to be vague, or individual PII beneficiaries are convinced their data is used solely to their advantage. *See* Kaufman, *supra* note 410; *see also* McQuinn *supra* note 406.

Comparing Opting: Opt-In vs. Opt-Out




413. Opt-out favors data collectors. *See, e.g.*, Kaufman, *supra* note 410.

414. *See* Delacroix & Lawrence, *supra* note 24, at 236 ("[T]here should be a plurality of Trusts, allowing data subjects to choose a Trust that reflects their aspirations, and to switch Trusts when needed.").

415. *See* Kaufman, *supra* note 410 (explaining that the United States currently operates as an opt-out regime, and though some states, including California, have opted for a hybrid opt-in and opt-out regime, many states have not, which may indicate that the United States is slow to move in adopting an opt-in regime).

preferences when authorized as an agent to deal with the many services required under US and state law to secure privacy preference opting, opt-in or opt-out, from their clients. Data trusts might execute the opting for their trustor-beneficiary clients. Thus, data trusts signal a shift to opt-in, but opt-out may not die out quickly. Indeed, existing data aggregators and brokers would conceivably resist opt-in. This reluctance could conceivably make their entry into the data trustee business unlikely without maintaining separate lines of business—one as data broker aggregator and another as data trustee. Arguably, data aggregators and data brokers may find it challenging to supply any abrupt and costly relationship change to take on fiduciary responsibilities (or gain the trust needed) to serve as data trustees.

### 2. Data Trusts' Deployment of Automated Negotiation

Detailed, multiple-term negotiations by automated contracting systems remain in their infancy.[416] Software is mostly deterministic, making trade-offs among essential terms in predictable ways according to preprogrammed protocols.[417] Despite the claims of electronic agent inventors that automated contracting is imminent, the parameters of selecting optimal tradeoffs between values of key terms (variables) may still require flexibility, currently performed best by human intervention.[418] However, as smart contracting matures (perhaps deploying distributed ledger technology),[419] automated negotiations may serve to significantly reduce transaction costs and expedite workable data trusts.[420] In addition, the potential for the standardization of such smart contracts could serve to vastly increase

416. *See supra* notes 389–93 and accompanying text (explaining the difficulty of implementing automated complex negotiations).

417. *See, e.g.*, Clack, *supra* note 388 (arguing standard, structured contract terms are needed in automated contracting).

418. *See, e.g.*, N.R. Jennings, P. Faratin, A. R. Lomuscio, S. Parsons, M. Wooldridge & C. Sierra, *Automated Negotiation: Prospects, Methods and Challenges*, 10 GRP. DECISION & NEGOT. 199, 208 (2001); *see also* SARIT KRAUS, *Automated Negotiation & Decision Making in Multiagent Environments*, *in* MULTI-AGENT SYSTEMS AND APPLICATIONS, 150, 153 (Jaime G. Carbonell & Jöorg Siekmann, eds., 2001).

419. *See, e.g.*, Scott J. Shackleford & Steven Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 YALE J.L. & TECH. 334, 342–43 (2017). A detailed discussion of the architecture or methods that smart contracts might use, some deploying distributed ledger forms of blockchain technologies, and some not, is well beyond the scope here.

420. SUSANNAH WILKINSON & JACQUES GIUFFRE, SIX LEVELS OF CONTRACT AUTOMATION: THE EVOLUTION TO SMART LEGAL CONTRACTS—FURTHER ANALYSIS 2 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3815445 [https://perma.cc/RL3W-NZW9].

the adoption of such technology in data trusts.[421] University of Chicago law professor Anthony J. Casey and University of Toronto law professor Anthony Niblett suggest that as AI technologies advance, micro-directives (a legal technology that uses AI-augmented algorithms to fill gaps and update contract provisions automatically) could create automated contracts.[422] Although algorithmic contracts are in use in various domains,[423] their legal effect remains to be determined.[424] The evolution and general recognition of either of these devices could mechanize and reduce costs of contracting and thereby help propel the acceptance and use of data trusts and make their operations more efficient.[425]

As more standardized contracts expedite data trust deployment and success, it seems likely that data trustee downstream contracts would be the most likely to be standardized. In some cases, costly human-negotiated agreements might be more appropriate downstream, such as with large or repeated data customers. Nevertheless, data trustees will likely seek automated negotiations to lower their transaction costs. It is difficult to predict when it may be possible for data trustee firms to use electronic agents to implement a digital privacy rights management system. Electronic agents could conceivably negotiate and enforce restrictions on the collection and use of data

---

421. *See generally* ARIANE GARSIDE, SUSANNAH WILKINSON, NATASHA BLYCHA & MARK STAPLES, DIGITAL INFRASTRUCTURE INTEGRITY PROTOCOL FOR SMART LEGAL CONTRACTS DIIP 2021 (2021) (proposing a set of requirements "for any high integrity digital infrastructure or Enterprise Platform (EP) intended to support Smart Legal Contracts: software-based legal contracts that are machine readable and have jointly-agreed coded instructions").

422. Anthony J. Casey & Anthony Niblett, *The Present and Near Future of Self-Driving Contracts*, *in* CAMBRIDGE HANDBOOK OF PRIV. L. & A.I. (forthcoming). The authors distinguish their "self-driving contracts" from distributed ledger technology smart contracts by explaining that their automated contracts would create substantive terms via algorithms, while a smart contract would merely execute automatically under certain conditions being met. *See id.* They do, however, acknowledge that others envision self-driving contracts as an advanced type of smart contract. *See id.* at 2 n.8.

423. Lauren Henry Scholz, *Algorithmic Contracts*, 20 STAN. TECH. L. REV. 128, 137, 141, 147 (2017) (describing current uses of algorithmic contracts in high frequency trading, dynamic pricing, and Ethereum blockchain transactions).

424. *Compare id.* at 128, 165–166 ("There is only a tenuous case for their enforceability under currently accepted approaches to contract law. The Uniform Electronic Transactions Act (UETA) was written and widely adopted nearly twenty years ago to make sure that contracts made electronically using basic automation techniques would be recognized as enforceable. However, the language of the UETA may be read to treat all putative contracts made with algorithms as properly formed, simply because they happen to be electronic."), *with* Matthew Oliver, *Contracting By Artificial Intelligence: Open Offers, Unilateral Mistakes, and Why Algorithms Are Not Agents*, 2 AUSTRALIAN NAT. U. J.L. & TECH. 45, 45 (2021) ("AI-negotiated contracts are enforceable within existing contract law doctrines [US and Australian]. We can explain why AI-negotiated contracts are enforceable by recognising that a person operating an AI contracting program make an open offer to contract on whatever terms the AI program agrees.").

425. *See generally* Mark Giancaspro, *Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective*, 33 COMPUT. L. & SEC. REV. 825 (2017).

automatically.[426] However, the concern would be the complexity accumulating to hundreds of variables in data onward transfers, the disclosure of data by any custodian in the information supply chain, envisioned for data trusts.[427] Automated negotiations become daunting when algorithms could vary the type of information restricted or made available, differentiate among classes of end users, impose timing restrictions, and force data expiration or expungement obligations on downstream users.[428] Until these technologies become reliable and commonplace, agreements may need to be made through simple click-through choices or costly negotiated agreements.[429]

## V. ANALYSIS AND SYNTHESIS

The need for greater control over personal data has spurred hundreds of recommendations, ranging from stricter privacy regulations to dismantling Big Tech.[430] This Article has explored data trusts as a solution. A trust arrangement offers benefits that other solutions do not.[431] Importantly, it takes the control over data out of the hands of Big Tech and places it into the hands of a fiduciary.[432] The beauty of the data trust concept is that data subjects can choose a trust aligned with their values and needs (e.g., individual privacy preferences or a desire to provide data for social good, such as medical research).[433]

---

426. *See* Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng & Muhamad Imran, *An Overview on Smart Contracts: Challenges, Advances and Platforms*, 105 FUTURE GENERATION COMPUT. SYS. 475, 475 (2020).

427. *See generally* Kuner, *supra* note 362.

428. *Id.* at 183.

429. Smart contracts and automated contracts are not without concerns. *See generally* PIETRO SIRENA & FRANCESCO PAOLO PATTI, *Smart Contracts and Automation of Private Relationships, in* CONSTITUTIONAL CHALLENGES IN THE ALGORITHMIC SOCIETY 315, 320 (Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor & Giovanni De Gregorio eds., 2021); Ben Chester Cheong & Harry Kishen, *Legal Risks Beneath Blockchain-Enabled Smart Contracts*, SING. L. GAZETTE (Jan. 2021), https://lawgazette.com.sg/feature/legal-risks-beneath-blockchain-enabled-smart-contracts/ [https://perma.cc/Z9TB-RCVY]; Marco Rizzi & Natalie Skead, *Algorithmic Contracts and the Equitable Doctrine of Undue Influence: Adapting Old Rules to a New Legal Landscape*, 14 J. EQUITY 301 (2020) (noting potential issues with consent and independent decision making that come along with algorithmic contracting).

430. *See generally* Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35 (2013).

431. *See* Anna Artyushina, *The EU is Launching a Market for Personal Data. Here's What That Means for Privacy*, MIT TECH. REV. (Aug. 11, 2020), https://www.technologyreview.com/2020/08/11/1006555/eu-data-trust-trusts-project-privacy-policy-opinion/ [https://perma.cc/9TJR-2H39].

432. *Id.* ("The single most important lesson from these revelations is that companies that trade in personal data cannot be trusted to store and manage it. Decoupling personal information from the platforms' infrastructure would be a decisive step toward curbing their monopoly power. This can be done through data stewardship.").

433. Delacroix & Lawrence, *supra* note 24, at 236.

As aptly stated by Delacroix and Lawrence, a data trust mechanism can "'give a voice' to data subjects whose choices when it comes to data governance are often reduced to binary, ill-informed consent."[434] The fiduciary obligation and independent data stewardship of the trustee can provide assurance to the data subjects that their interests will predominate over the interests of the data users.[435] Both data leakage and derived data harms are mitigated by limiting data use to only that which is authorized and stated directly in the terms of the data trust.[436] Another data trust design option might be to permit the sharing of data to SMEs, nonprofits, and academics bringing about new innovations and social good.[437] They also provide the potential for the compensation of the data subjects in line with the terms of the trust.[438]

Cross-border transfers between the European Union and United States have been impeded by the invalidation of the Privacy Shield and by regulatory actions brought against US technology companies by data protection authorities in the European Union.[439] Impeded data movement across borders stands to inhibit the data fugacity needed for the success of data trusts as envisioned here.[440] It is unlikely that ideological differences around privacy between the two regions will be resolved anytime soon. Because this relationship is very important to both the European Union and United States, a device which will protect personal data and meet the requirements for "adequate measures"

---

434. *Id.*

435. *See id.*

436. Zhang, *supra* note 251 (explaining that data trusts provide a way to both balance privacy with data utility and recommending that key technologies be explored to provide (1) privacy protected data release, (2) blockchain technology to trace data circulation, and (3) privacy-protected federated learning). For an explanation of how a data trust could incorporate blockchain that "promotes data quality by assessing input data sets, effectively manages access control, and presents data provenance and activity monitoring," see Rouhani & Deters, *supra* note 158.

437. *See generally* Anastassia Lauterbach, *Unitarism vs. Individuality and a New Digital Agenda: The Power of Decentralized Web*, 3 FRONTIERS HUM. DYNAMICS (2021).

438. There is some disagreement in the literature as to whether compensating data subjects who provide their data to a trust is appropriate. ELEMENT AI & NESTA, *supra* note 232, at 25 (discussing the alternatives of charging a license fee to data users versus state funding). *Compare* Geoff Mulgan & Vincent Straub, *The New Ecosystem of Data Trusts*, MEDIUM (Feb. 26, 2019), https://medium.com/@vincejstraub/the-new-ecosystem-of-data-trusts-36901fc59010 [https://perma.cc/87BM-RRMZ] (suggesting payments to data subjects), *with* George Iacovou, *What Is a Data Trust?*, INCOGNITO BY METOMIC (Sept. 6, 2019), https://medium.com/metomic-in-cognito/what-is-a-data-trust-9eb8fe927873 [https://perma.cc/VQ78-323Y] (quoting Mozilla data trust scholar, Anouk Ruhaak, as promoting data trusts as not-for-profits).

439. *See* Stucke, *supra* note 15.

440. ARCHICK & FEFER, *supra* note 107, at 20–22 (arguing dislocation of US data intensive industries without freer international data flows).

under the GDPR will provide immediate benefits.[441] According to the Information Technology and Innovation Foundation,

> A clear, predictable, and accessible legal framework for data protection makes it easier for organizations to manage and transfer data. Transatlantic data flows allow firms from all sectors to benefit from data-driven innovation, strengthen trade between countries in a growing range of digital and digitally-enabled goods and services, and expand consumers' access to a growing variety of goods and services. The EU-[US] Privacy shield was especially important to enable [SMEs] on both sides of the Atlantic to transfer data abroad because they don't have the resources or expertise to use other more costly and complicated legal mechanisms.[442]

Although there are different legal issues surrounding the use of data trusts arising from jurisdictional differences, it appears that the European Union may be on track to include data trusts as a data sharing mechanism under the Data Governance Act.[443] This would permit US companies to more easily access data from the European Union should they employ the use of data trusts.[444] There is also some debate as to whether the GDPR needs to be updated to expressly permit the secondary use of data for the development of AI.[445] Article 6(4) of the GDPR permits processing for secondary uses, provided they are compatible with the purpose for which the data is collected, and the implementation of appropriate safeguards, which may include the anonymization or pseudonymization of the data.[446] There is also some concern over whether data can be transferred to a trust and whether

---

441. *See supra* notes 96–107. Neither AI nor data trusts can be expected to operate well without free movement of data across borders, making the international harmonization of some privacy rights foundational to success. *See id*.

442. Nigel Cory, Daniel Castro & Ellysse Dick, *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, INFO. TECH.Y & INNOVATION FOUND. (Dec. 3, 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic [https://perma.cc/2KGT-EJY9] (citations omitted).

443. Jess Montgomery, *Data Trusts and the Draft of the Data Governance Act*, DATA TRS. INITIATIVE (2021) https://datatrusts.uk/blogs/data-trusts-and-the-draft-data-governance-act [https://perma.cc/TB55-5XVT].

444. *See supra* notes 96–100.

445. *See generally supra* Section II.C. Those very involved in data trusts do believe that they are permissible under the GDPR to protect the rights given to data subjects in the EU. *See* DELACROIX & MONTGOMERY, *supra* note 233, at 11; Zarkadakis, *supra* note 164. Data trusts and AI have similar needs for both domestic and international data flows. *See id*.

446. Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) (EU) [GDPR] provides:

> Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia . . . (e) the existence of appropriate safeguards, which may include encryption or pseudonymization.

subjects may delegate their rights to a trustee.[447] Some have suggested that Article 80 of the GDPR, which permits data subjects to delegate their right to lodge a data complaint to certain organizations, would need to be expanded to permit data subjects to delegate their data rights to a trustee (or that further regulatory guidance be issued regarding such delegation).[448] The ability to delegate in Article 80 appears to only apply to complaint proceedings.[449] However, Germany appears open to the use of data trusts to "help individuals take control over data about them and foster competition in data-driven markets."[450] It is possible that member states can craft their own regulations so as to promote, or at least permit, the use of data trusts in compliance with the GDPR.

In the United States, data trusts present a different issue. Except as preserved in a few state laws,[451] people have very few data rights. It would be difficult to argue that "data rights" can comprise trust property because, except in very few circumstances, these rights do not exist. The trust res issue—concerning the property status of data—appears to be less contentious in the United States.[452] The Director of the Digital Governance Design Studio at Duke Law, Keith Porcaro, suggests that "any property, whether digital or not" can be

447. *See* ANOUK RUHAAK, DATA TRUSTS IN GERMANY AND UNDER THE GDPR 13–15 (Dec. 6, 2020), https://algorithmwatch.org/en/data-trusts-germany-gdpr/ [https://perma.cc/94K4-7HXN].

448. *Id*.

449. *Id*.; *see also* Delacroix & Lawrence, *supra* note 24, at 247–48.

450. ALINE BLANKERTZ, DESIGNING DATA TRUSTS 5 (2020), https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf [https://perma.cc/843F-ZHUP].

451. *See State Laws Related to Digital Privacy*, NAT'L CONF. STATE LEGIS. (June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/78P3-7DW9]. Consumer privacy laws will become effective in California, Colorado, and Virginia in 2023. *See* California Privacy Rights Act (CPRA), CAL. CIV. CODE § 1798.185(d); Colorado Privacy Act (CPA), S.B. 21-190, 73d Leg., 2021 Reg. Sess. (Colo. 2021), to be codified in Colo. Rev. Stat. ("C.R.S.") Title 6; and Virginia Consumer Data Protection Act (VCPDA), S.B. 1392 § 59.1–571.

452. Recently, American Airlines was able to use its airline loyalty program as collateral for a $5.5 billion dollar loan. The database of information on its customers was valued at between $18 and $30 billion. This would seem to indicate some recognition of data as property. *See generally* Gary Leff, *American Airlines Just Mortgaged the AAdvantage Frequent Flyer Program for $5.5 Billion*, VIEW FROM WING (Sept. 25, 2020), https://viewfromthewing.com/american-airlines-just-mortgaged-the-aadvantage-frequent-flyer-program-for-5-5-billion/ [https://perma.cc/N2JT-VZKY]; *see also* Hazel, *supra* note 257 (arguing Demsetz's formula favors the creation of property rights in personal data); Paulius Jurcys, Christopher Donewald, Mark Fenwick, Markus Lampinen, Vytautas Nekrošius & Andrius Smaliukas, *Ownership of User-Held Data: Why Property Law Is the Right Approach*, HARV. J.L. & TECH. DIG. (Sept. 21, 2021), https://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach#:~:text=We%20show%20that%20user%2Dheld,and%20can%20be%20freely%20alienated. [https://perma.cc/UPR4-DMJ2] (arguing that individuals should own their user-held data). Rapidly developing data processing technologies empower individuals to collect their data from different sources and retain it in personal data clouds. *See id.* Such user-held data represents the most accurate, up-to-date, and rich information about the individual. *See id.*

trust property.[453] The issue he sees is whether or not the fungibility and representative nature of data present practical issues for trust management.[454] However, there does seem to be some precedent in the United States for holding data in a trust.[455] The Department of Transportation has provided guidance in this regard on the use of data trusts to hold transportation information.[456] However, until the trust res issue is resolved and legal rights are established for data subjects in the United States, which would include data portability (enabling the transfer of data among trusts), the right to delegate data to a trust (circumventing the ability of Big Tech to control the data), and limits on data use (preventing Big Tech from using data in a way that harms data subjects prior to directing it to a trust), the data trust concept may not catch on. Although neither an omnibus privacy law nor a designation of data as the property of the data subject is likely to be enacted anytime soon by the federal government, state legislatures could employ these rights.[457]

One of the most important practical aspects of any type of governance mechanism is the balancing of data subject rights and protections with the value creation available from these sets of data.[458] If restrictions on data users are too tight, there is little incentive for them to contract with the trustee.[459] If the restrictions on data use are too loose, data subjects will not see the utility of providing their data to the trust.[460] However, data trust co-design can address this. Rather than utilize a standardized form, because data trusts can be designed

453. Porcaro, *supra* note 228, at 335–36 ("Any property can be trust property, digital or not. Whether data, especially personal data, should be considered property is the subject of continued debate. We need not resolve the issue here. For our purposes, it is sufficient to ask whether it is possible to represent a given dataset in terms of ascertainable property interests (we can obviously do so for code and other digital assets). Under current law, with some exceptions, the answer is generally yes. A specific instance of data—a database stored on a server or a cloud service—can be ascertainable as property. So too could the rights to access or query a data source or a continuing stream of data be considered trust.") (citing RESTATEMENT (THIRD) OF TRUSTS, §§ 40–41 (AM. L. INST. 2003)).

454. *Id*. at 336.

455. *See* U.S. DEP'T OF TRANSP., ORDER NO. 1371.1, DATA TRUST POLICY, GUIDELINES AND PRINCIPLES 1–2 (Jan 28, 2020).

456. *Id.*; *see also* KRISTI MILLER, AN OVERVIEW OF TRANSPORTATION DATA 1 (2018), https://static.tti.tamu.edu/tti.tamu.edu/documents/PRC-2018-2.pdf [https://perma.cc/UVN8-HS22] (describing the importance of transportation data and indicating that it is "collected and managed as an asset").

457. The CCPA contains a delegation provision which would seem to consider the use of a data trust, at least with respect to certain rights held by data subjects under the CCPA. *See, e.g.*, CAL. CODE REGS. tit. 11, § 7001(c), § 7063 (2022).

458. Xiaolan Yua & Yun Zhao, *Dualism in Data Protection: Balancing the Right toPersonal Data and the Data Property Right*, 35 COMPUT. L. & SEC. REV., no. 5, 2019, at 1, 8.

459. *See* Delacroix & Lawrence, *supra* note 24, at 236.

460. *See id.*

in an indeterminable number of configurations,[461] Ostrom's work is instructive here. Ostrom's eight design principles can be used as a framework to ensure proper governance is built in to data trusts: (1) *Clearly defined boundaries* would require the identification of the parties, the type of data collected, and the rights and obligations of the parties; (2) *congruence between appropriation and provision rules and local conditions* would be reflected in the creation and management through the trustee of the data that could potentially involve rewards for the data subjects for the use of their data; (3) *collective-choice arrangements* would require that input from all stakeholders be considered in the creation of the trust; (4) *monitoring* would involve the securing and auditing of data and its use by data users; (5) *graduated sanctions* would be built into the trust document to ensure that violations could be detected and punished (building up to potential fines and withdrawal of access); (6) *conflict resolution mechanisms* would enable disagreements to be handled prior to the unsanctioned use of data or withdrawal of data subjects; (7) *minimal recognition of rights to organize* would be incorporated through the boundaries set in design principle (1) above and would require consideration of the data laws in the jurisdiction in which the data subjects are located, and (8) *nested enterprises* would necessitate the development of standards regarding the data and require the ability to move data from one trust to another (interoperability).[462]

In addition, the modes of contracting for data trusts span at least three, if not more, streams. Unnegotiable, click-through, opt-in recruitment upstream for data acquisition appears most likely in data subject-trustor-beneficiary relations. Cross-stream retention of service providers would likely require traditional contracting, unless and until automated negotiation proves itself. Downstream-access licenses to third parties could either be automated or negotiated. As such, the viability and enforceability of data trust contracting, especially with respect to automated, algorithmic, or smart contracting, would need to be resolved.[463] Finally, contract enforceability of international cloud service may require more careful consideration.[464]

Interestingly, the proposed US ACCESS Act would require platform interoperability to ensure data portability, which would be

---

461. *See generally* NEIL LAWRENCE, SEONGTAK OH, ENABLING DATA SHARING FOR SOCIAL BENEFIT THROUGH DATA TRUSTS (2021), https://gpai.ai/projects/data-governance/data-trusts/enabling-data-sharing-for-social-benefit-data-trusts-interim-report.pdf [https://perma.cc/EYR7-J3Z3].

462. Extrapolating from OSTROM, *supra* note 183, at 532 (Chapter 36).

463. *See supra* Section IV.C.

464. *See* Bernard H. Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555, 556 (2021) (arguing privacy rights are illusory without available remedies for breach of contract).

critical for data subjects to be able to move from one trust to another and for the facilitation of access to the trust res.[465] Although the investigation of data trusts is further along abroad, US states may be able to create a friendly regulatory environment for them, much in the same way that California has created state privacy protections—in the CCPA—based on the GDPR, more quickly than either the federal government or the European Union.[466]

## VI. CONCLUSION

Data trusts offer a potential solution to the oversharing of data by Big Tech, resulting in harms to data subjects,[467] and the under-sharing of data from Big Tech to smaller commercial entities[468] and those interested in using data for social good.[469] Because access to large data sets is so important for the growing use of AI and the increase in cross-border data sharing, data trusts offer an opportunity to surmount the barriers and difficulties created by different data use regimes.[470] As the world wrestles with how to address Big Tech and governments begin to realize that there is no one perfect regulation to rule them all, data trusts can serve as a flexible, broad-based governance solution to data sharing problems, permitting customization to address stakeholder needs.

465. Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021, H.R. 3849, 117th Cong. (2021); *see also* Cyphers & Doctorow, *supra* note 144 (arguing that removing the "delegability" requirement that was present in the 2019 version from the Act makes it less effective).

466. *See, e.g.*, CAL. CODE REGS. tit. 11, § 7001(c), § 7063 (2022).

467. *See supra* Section II.A.

468. *See supra* Section II.C.

469. *See supra* Section II.D.

470. *See supra* Section II.B.