DATA TYPES, DATA DOUBTS & DATA TRUSTS

JOÃO MARINOTTI*

Data[1] *is not monolithic. Nonetheless, the word is frequently used indiscriminately—in reference to a number of distinct concepts. It may refer to information writ large, or specifically to personally identifiable information, discrete digital files, trade secrets, and even to sets of AI-generated content. Yet each of these types of "data" requires different governance regimes in commerce, in life, and in law. Despite this diversity, the singular concept of data trusts is promulgated as a solution to our collective data governance problems. Data trusts—meant to cover all of these types of data—are said to promote personal privacy, increase corporate transparency, facilitate the sharing of data, and even pave the way for the next generation of artificial intelligence. These anticipated benefits, however, require the body and flexibility of equitable trust law and its inherent fiduciary relationships for their fruition. Unfortunately, American trust law does not allow for the existence of such general data trusts. If anything, the judicial, academic, and legislative confusion regarding data rights—or data's status as property—demonstrates that discussions of data trusts may be ignoring a key element. Without first determining whether (or what kind of) data can be recognized as a trust* res *(i.e., as trust property) under existing law, it may be premature to accept data trusts as the private law solution to data governance. If, on the other hand, the implementation of data trusts requires legislative intervention, its purported benefits must be analyzed in contrast to the myriad other new and evolving data governance frameworks that would similarly require legislation. By analyzing existing trust law and the difficulties of defining data rights, this essay highlights the urgent need to pursue doctrinally, legislatively, and technologically viable data governance strategies.*

 Associate Professor of Law at Indiana University Maurer School of Law; Affiliated Fellow at Yale Law School Information Society Project; Fellow at Indiana University Center for Intellectual Property Research; Research Affiliate at the Program on Data Governance and Information Management at the Ostrom Workshop. Many thanks to the Data Trust working group at the Ostrom Workshop. And many thanks to the students in my Spring 2020 Seminar on Rethinking Thinghood for their engaging thoughts on property theory and to Kazumasa Watanabe for great work as a research assistant.

[1] The concept of data is referred to as a singular mass noun throughout this essay. While historically, data was the plural of datum, the term evolved semantically and syntactically. *See Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data [https://perma.cc/JF6B-CPMY] ("*Data* leads a life of its own quite independent of *datum* . . . . It occurs in two constructions: as a plural noun (like *earnings*) . . . ; and as an abstract mass noun (like *information*), taking a singular verb . . . and being referred to by a singular pronoun (*it*). Both constructions are standard.").

INTRODUCTION

From the ongoing COVID-19 pandemic,[2] to the George Floyd protests,[3] to the Capitol riot of January 6, 2021,[4] the early 2020s have been unprecedented. In one specific way, however, it has been business as usual. Meta, Alphabet, TikTok, and T-Mobile, among many other global tech giants, were sued, investigated, and/or fined in jurisdictions across the world due to their data practices.[5] Such lawsuits are not unexpected. In the era of surveillance capitalism,[6] it is no wonder that these companies collect, use,

---

[2] *See Two Years of the Pandemic in New York, Step by Awful Step*, N.Y. TIMES (Mar. 15, 2022), https://www.nytimes.com/interactive/2022/nyregion/nyc-covid-timeline.html [https://perma.cc/AK7A-9LY7].

[3] *See* Derrick Bryson Taylor, *George Floyd Protests: A Timeline*, N.Y. TIMES (Nov. 5, 2021), https://www.nytimes.com/article/george-floyd-protests-timeline.html [https://perma.cc/DWW5-PJKZ].

[4] *See* Kat Lonsdorf, Courtney Dorning, Amy Isackson, Mary Louise Kelly & Ailsa Chang, *A Timeline of How the Jan. 6 Attack Unfolded – Including Who Said What and When*, NPR (June 9, 2022), https://www.npr.org/2022/01/05/1069977469/a-timeline-of-how-the-jan-6-attack-unfolded-including-who-said-what-and-when [https://perma.cc/8VPZ-2T5Q].

[5] *See, e.g.*, Cecilia Kang, *Mark Zuckerberg Will Be Added to a Facebook Privacy Lawsuit*, N.Y. TIMES (Oct. 29, 2021), https://www.nytimes.com/2021/10/20/technology/mark-zuckerberg-facebook-lawsuit.html [https://perma.cc/AE5W-J9ZM] (describing a lawsuit alleging that "Facebook misled consumers about privacy on the platform by allowing Cambridge Analytica, a political consulting firm, to obtain sensitive data from more than 87 million users, including more than half the district's residents"); Jessica Davis, *Google Sued, Lawsuit Claims COVID-19 Contact Tracing Tool Exposes Data*, HEALTH IT SEC. (Apr. 30, 2021), https://healthitsecurity.com/news/google-sued-lawsuit-claims-covid-19-contact-tracing-tool-exposes-data [https://perma.cc/5NR5-HHQY] (describing a lawsuit alleging that Google exposed contact tracing app "participants' private personal and medical information associated with contact tracing" to "dozens or even hundreds of third parties"); Bobby Allyn, *TikTok to Pay $92 Million to Settle Class-Action Suit Over 'Theft' of Personal Data*, NPR (Feb. 25, 2021), https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data [https://perma.cc/2W4K-3UWR] (describing the settlement of a lawsuit alleging that TikTok, "the popular video-sharing app[,] harvested personal data from users, including information using facial recognition technology, without consent and shared the data with third-parties, some of which were based in China"); Jake Holland, *T-Mobile Hit with Class Action Suits After Consumer Data Breach*, BLOOMBERG L. (Aug. 20, 2021), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X66IAT24000000 [https://perma.cc/2LSA-638M] (describing a lawsuit alleging that T-Mobile was negligent and "violated the CCPA by failing to prevent consumers' nonencrypted personally identifiable information 'from unauthorized access and exfiltration, theft, or disclosure'").

[6] *See generally* Donell Holloway, *Explainer: What Is Surveillance Capitalism and How Does It Shape Our Economy?*, THE CONVERSATION (June 24, 2019) https://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-

and abuse the nearly endless amount of data we willingly hand over for what have become indispensable and/or free services. Without being held sufficiently financially accountable for data malfeasance,[7] these companies have few reasons to protect or prioritize our privacy and data security over their singular—and legally legitimate—duty to maximize shareholder value.[8] From this point of view, underinvesting in cybersecurity and failing to meet even the most basic of inform-and-consent privacy policies may be a successful business practice in today's regulatory environment.[9]

At the end of 2020, a federal judge offered a prime example of this lack of accountability in a case against Facebook.[10] Without disclosure or consent, Facebook used customers' IP addresses to sell localized advertisements. In dismissing the class action complaint, Judge James Donato explained that "[t]here is no legally protected privacy interest in IP addresses," so plaintiffs "cannot be injured from the collection of IP addresses, and so lack Article III standing for the privacy claims under California common law, the California constitution, and [the California Invasion of Privacy Act] that are premised on that ostensible injury."[11] The judge further clarified that plaintiffs "also lack Article III standing for the unjust enrichment claim because they have failed to make any allegation that 'they retain a stake in the profits garnered from' the collection of their IP addresses."[12] Legally and financially, then, was Facebook right to collect and profit from this consumer

---

our-economy-119158 [https://perma.cc/S5P9-BLAV] (explaining surveillance capitalism as "a market driven process where the commodity for sale is your personal data, and the capture and production of this data relies on mass surveillance of the internet").

7 *See, e.g.*, Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1004 (2018) ("[O]ur legal system has not yet created adequate incentives for individual companies to take the necessary—and sometimes costly—steps to reduce the likelihood of cybersecurity attacks."); Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 100 (2020) ("The current state of cybersecurity regulation is often described as a 'patchwork' of laws at federal and state levels that lack the sort of coordination and coherence necessary to effectively promote the security of our connected technologies.").

8 *See* Vagle, *supra* note 7, at 103 ("[T]echnology companies often choose to shave their development costs by reducing or eliminating resources necessary to support secure software development."); *see also* Felicia R. Resor, *Benefit Corporation Legislation*, 12 WYO. L. REV. 91, 95 (2012) ("The shareholder wealth maximization norm, derived from state corporate law and national corporate norms, stands for the proposition that directors have a duty to maximize shareholder wealth. . . . [D]irectors can be held liable for not doing so."); Robert J. Rhee, *A Legal Theory of Shareholder Primacy*, 102 MINN. L. REV. 1951, 2010 (2018) ("Courts have imposed the obligation of shareholder primacy on the entire spectrum of managerial decisions.").

9 Robert H. Sloan & Richard Warner, *How Much Should We Spend to Protect Privacy: Data Breaches and the Need for Information We Do Not Have*, J.L. ECON. & POL'Y, Winter 2018, at 119, 121–22 ("Organizations have insufficient incentives to invest in strong data security . . . . [L]ost or 'stolen' customer or employee data often does not deprive an organization of its continued availability or use . . . . Further, the (negative) consequences of poor security and misused data fall mainly if not entirely upon individual victims.").

10 Heeger v. Facebook, 509 F. Supp. 3d 1182, 1190 (N.D. Cal. 2020).

11 *Id.*

12 *Id.* at 1191.

data even without the proper informed consent? Its shareholders certainly must think so.[13]

Even when companies are unquestionably at legal fault, the victims of data malfeasance are frequently unable to receive adequate compensation, if anything at all. The Equifax data breach of 2017 comes to mind as a prime, and infamous, example. The names, birthdates, and social security numbers of over 147 million Americans were exposed due to the company's mismanagement.[14] Yet, if every victim claimed a portion of the allotted settlement, each individual would receive roughly only twenty-one cents![15] Such settlements neither affect the business practices of these global giants,[16] nor do they provide adequate remedies for the victims harmed. If these consequences neither deter future cyber-negligence nor compensate victims for harms experienced, what, then, are they for? Unfortunately, some argue they are "mostly exercises in public relations," remediating the reputation of both regulators and companies alike.[17]

Given the evidence that existing systems of data governance insufficiently incentivize privacy, cybersecurity, and respect for individual data autonomy, it is not surprising that various alternate means of data governance are being actively researched.[18] In this Essay, I seek to examine one such proposal that is gaining steam in academic and policy circles alike:

---

13 The underinvestment in cybersecurity and privacy need not always be attributed to malice or negligence. "[I]nsights from behavioral economics and psychology show that human judgment is often biased in predictably problematic ways," which causes companies to "treat cybersecurity as a finite problem that can be solved, rather than as the ongoing process that it is." Alex Blau, *The Behavioral Economics of Why Executives Underinvest in Cybersecurity*, HARV. BUS. REV. (June 7, 2017), https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity [https://perma.cc/YQ96-DAN8].

14 Alvaro Puig, *Equifax Data Breach Settlement: What You Should Know*, FTC: CONSUMER ADVICE (July 22, 2019), https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know [https://perma.cc/CBG2-CMPN].

15 Shahar Ziv, *Here's Why You Could Get as Little as $0.21 from Equifax's Data Breach Settlement*, FORBES (Aug. 1, 2019), https://www.forbes.com/sites/shaharziv/2019/08/01/you-might-only-get-21-cents-from-the-equifax-data-breach-settlement-instead-of-125 [https://perma.cc/75HA-KPPE].

16 *See* Jonathan Trebble-Greening, *Raising the Stakes: Creating an International Sanction to Generate Corporate Compliance with Data Privacy Laws*, 2019 COLUM. BUS. L. REV. 763, 778 (2019) ("The fines . . . on companies . . . may not effectively alter corporate actions . . . [because] companies like Google and Facebook earn exceedingly high revenues that current fines . . . do not dent corporate coffers enough to create the deterrent effect.").

17 Jason Aten, *Equifax Promised It Would Give You $125. Then It Made It Clear That Was Never Going to Happen. Here's What You Should Do Now*, INC. MAG. (Sept. 17, 2019), https://www.inc.com/jason-aten/equifax-promised-it-would-give-you-125-then-it-made-it-clear-that-was-never-going-to-happen-heres-what-you-should-do-now.html [https://perma.cc/32VH-2T6D].

18 *E.g.*, Marina Micheli, Marisa Ponti, Max Craglia & Anna Berti Suman, *Emerging Models of Data Governance in the Age of Datafication*, BIG DATA & SOC'Y, July–Dec. 2020, at 1, 6 (examining four such models of data governance: data sharing pools (DSPs); data cooperatives (DCs); Public Data Trusts (PDTs); and Personal Data Sovereignty (PDS)).

the data trust.[19] While acknowledging the importance of such research, I aim to highlight potential doctrinal hurdles that may impede the successful adoption and implementation of data trusts in the United States. In doing so, I do not aim to shut down the conversation; rather, I seek to raise a set of fundamental questions that must be dealt with for the successful adoption and implementation of the model as a useful private law solution to our data governance concerns.

This Essay proceeds in three parts. Part I discusses the relationship between trust law and fiduciary duties. In so doing, it highlights why the concept of data trusts requires doctrinally valid equitable trusts to sufficiently protect personal privacy and individual autonomy in an ever-evolving technological landscape. Part II dissects trust doctrine to distill the rationales behind the requirement of an ascertainable and definable trust property. By juxtaposing these rationales with existing attempts to define and protect data, the Essay highlights the difficulties any court would encounter in its attempt to recognize data as trust property under existing law. Finally, Part III builds on this analysis to question whether data trusts are truly able to fulfill what many of their advocates desire: immediate private implementation. It argues that legislative intervention is nonetheless required for the implementation of data trusts. The Essay concludes that data trusts should only be legislatively pursued, however, if they offer advantages over the myriad other new and evolving data governance frameworks that would also require legislative action.

I
TRUST LAW & FIDUCIARY DUTIES

To adequately discuss the nuances and potential problems of data trusts, it is first necessary to highlight another governance strategy: the strategy of information fiduciaries.[20]

A. Information Fiduciaries

To hold global tech giants more accountable, Professors Jack Balkin and Jonathan Zittrain proposed a revolutionary solution based on an ingenious and, in retrospect, obvious, observation. While their ideas would require drastic—and potentially unlikely—legislative intervention in the face of federal gridlock, the theory pushed for the introduction of fiduciary

---

19 *See infra* notes 32–36 and accompanying text. *See generally infra* Part II.

20 *See generally* Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/RL3R-PERF]; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020).

duties in the context of "huge online businesses, like Facebook, Google, and Uber, that collect, analyze, and use our personal information."[21]

Balkin and Zittrain noted that in many ways, global tech giants resemble doctors, lawyers, and accountants. Much like the Googles of the world, these professionals "know so much about us."[22] Thankfully, though, "because we have to depend on [such professionals], the law requires them to act in good faith—on pain of loss of their license to practice, and a lawsuit by their clients."[23] They "have to keep our secrets and they can't use the information they collect about us against our interests."[24] This legal relationship between clients and their doctors, lawyers, and accountants is a *fiduciary* one. These professionals have a fiduciary duty to their clients; they have a "duty to act with due regard for the interests of another" (i.e., their clients).[25] This fiduciary duty legally prevents them from abusing the sheer quantity of sensitive information at their disposal. Acknowledging the similarities between these professionals and the tech giants, Balkin and Zittrain asked in 2016 why these global giants are not treated as "information fiduciaries."[26] Under this designation, tech companies would have legal obligations to prioritize consumer privacy and data protection over profit—they would be required to act with due regard for the interests of their consumers.

In spite of its conceptual attractiveness and broad support from organizations like the Electronic Frontier Foundation (EFF),[27] the idea of information fiduciaries has yet to be implemented in state or federal law. And given the current political climate and legislative gridlock, it is unlikely that any federal information fiduciary law or any other comprehensive federal data privacy framework will be adopted in time to prevent the further abuse of our personal information.[28]

Recently, alternative means of creating fiduciary relationships have been explored. One of these may even bypass the legislative process by

---

21 Balkin & Zittrain, *supra* note 20.

22 *Id.*

23 *Id.*

24 *Id.*

25 Pagliara v. Johnston Barton Proctor & Rose, LLP, 708 F.3d 813, 818 (6th Cir. 2013).

26 Balkin & Zittrain, *supra* note 20.

27 Adam Schwartz & Cindy Cohn, *"Information Fiduciaries" Must Protect Your Data Privacy*, ELEC. FRONTIER FOUND. (Oct. 25, 2018), https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy [https://perma.cc/EW57-AKMM].

28 For example, the Data Care Act sponsored by Senator Schatz would have established fiduciary duties for online providers but died in the Senate in 2019. *See Schatz Leads Group of 15 Senators in Introducing New Bill to Help Protect People's Personal Data Online*, U.S. SENATOR FOR HAWAI'I BRIAN SCHATZ (Dec. 12, 2018), https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online [https://perma.cc/X6PS-X64B].

tapping into an existing area of private law: the law of trusts.[29] In the United States, a trust is a legal relationship in which one party, the trustee, holds and manages assets for the benefit of another party, the beneficiary. Notably, a trust relationship can be created privately by merely transferring assets to the designated trustee.[30] In a data trust, then, data would be "placed under the control of a board of trustees with a fiduciary responsibility to look after the interests of the beneficiaries."[31] This responsibility would be similar to, if not the same as, the fiduciary duties promoted by Balkin and Zittrain, but without the need for legislative action.

The idea of private data trusts[32] is gaining traction in academic centers, nonprofits, and think tanks around the world, like the Centre for International Governance Innovation and the Ostrom Workshop, among many others.[33]

---

29 *See, e.g.*, Lisa M. Austin & David Lie, *Safe Sharing Sites*, 94 N.Y.U. L. REV. 581, 618 (2019) ("Instead of waiting for the slow process of law reform to create such a regulatory framework, the trust model offers a way of managing these emerging issues through a private law mechanism.").

30 RESTATEMENT (THIRD) OF TRUSTS § 20 (AM. L. INST. 2003) ("Except as required by a statute of frauds, a writing is not necessary to create an enforceable inter vivos trust, whether by declaration, by transfer to another as trustee, or by contract.").

31 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/7ESV-9ZBZ]. *See also* Ira S. Rubinstein & Bilyana Petkova, *Governing Privacy in the Datafied City*, 47 FORDHAM URB. L.J. 755, 809–10 (2020) ("For example, a group of Fitbit and Apple Watch users might agree to pool their medical data in a data trust with explicit terms for how the trustee may share the data for medical research purposes—subject to various limitations set out in advance, and to the trustee's independent judgment of which uses uphold the interests of the users."). For a more thorough discussion of trust law, see generally *infra* Section I.B.

32 In this article, I discuss data trusts in their nominal form, meaning common law trusts over data. Commentators in this field have broadened the meaning of the term to include merely conceptually-similar data-management regimes, whether private or public, though such usages will not yield trust-derived fiduciary duties under existing law. *See, e.g.*, Richard S. Whitt, *Hacking the SEAMs: Elevating Digital Autonomy and Agency for Humans*, 19 COLO. TECH. L.J. 135, 184 (2021) ("A *data trust* is based on collective agency over the personal data and information of a specified collective of individuals. Here the entity manages a pool of data on behalf of a community of individuals."); Kimberly E. Diamond, *The Yoga Analogy: Scaling-Up the US's Renewable Energy Sector Mindfully with New Technologies, Evolving Standards, Public Buy-In, Data Sharing, and Innovation Clusters*, 32 FORDHAM ENV'T L. REV. 381, 474–75 (2021) ("A 'data trust' is a construct that allows multiple organizations within the public-private partnership to access shared data anytime . . . . A data trust not only functions as a relationship builder and a catalyst for action, but it also presents a legal framework that facilitates data sharing among member partners.").

33 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/BKF7-FZQC]; Digit. Civ. Soc'y Lab, *A Framework for Data Trusts*, STANFORD CTR. ON PHILANTHROPY & CIV. SOC'Y (Mar. 28, 2019), https://pacscenter.stanford.edu/research/digital-civil-society-lab/a-framework-for-data-trusts [https://perma.cc/NFZ3-4EM5]; MOZILLA INSIGHTS, JONATHAN VAN GEUNS & ANA BRANDUSESCU, SHIFTING POWER THROUGH DATA GOVERNANCE 13–14 (2020), https://assets.mofoprod.net/network/documents/ShiftingPower.pdf [https://perma.cc/4V5W-A4XT]; Ostrom Workshop, *Addressing Data Management & Information Governance*, IND. UNIV., https://ostromworkshop.indiana.edu/research/data-management/index.html [https://perma.cc/6YD5-VGB4].

According to the proponents of data trusts, this method of governance is beneficial for a number of reasons above and beyond its built-in fiduciary duties. The following three considerations highlight the range of such proposed benefits. First, data trusts are said to promote "the beneficial use of data" by "pooling data from various sources together" and "unlock[ing] the ability for a data trustee to negotiate on behalf of the collective, rather than an individual," functioning much like a labor union but in the context of data.[34] Second, data trusts purportedly "could make it much easier for firms to safely share data," promoting the creation of next-generation AI applications by addressing "the scarcity of varied, high-quality raw data."[35] And third, by using a data trust, a company may potentially be seen as more trustworthy by establishing a structure that gives users "granular visibility and control" into how their data is accessed, used, and managed.[36] Although the validity of these claims is outside the scope of this short Essay, it is clear that data trusts are currently being explored as one of the most powerful and viable private law solutions to the current struggles in data protection and privacy. One technical but significant problem, however, is that the private law of trusts in various American jurisdictions may not currently allow the creation of a data trust at all.

B. The Data "Trust"

Before diving into American trust law, what it requires, and how it may (or may not) apply to data, it is useful to demonstrate what American trust law is not. For this, we can compare it with German law, in which a trust arrangement is merely a contractual obligation.[37] In such an arrangement, the roles of data generator, data manager, and data beneficiary[38] may be contractually defined, allocated, and enforced. One such arrangement was entered into by Microsoft Germany, whereby an independent corporation called T-Systems served as the contractual data trustee and "significantly

---

34 Ruhaak, *supra* note 31 (emphasis omitted).

35 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/PL66-RRYW]. ("[A] data trust can guarantee transparency . . . as well as auditing of who is using the data at any time and for what purpose . . . thus removing the considerable legal and technological friction that currently exists in data sharing.").

36 *What Is a Data Trust? Everything You Need to Know*, SIGHTLINE INNOVATION, https://docs.sightlineinnovation.com/dtaas/overview.html#what-is-a-data-trust [https://perma.cc/H6UL-VZBJ] (explaining data trusts decouple "the problem of cataloging, managing, and sharing data assets from the problem of generating, viewing, and interacting with them").

37 *See* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1698 (2018).

38 For example, a corporation compiling raw but machine-readable data would be the data generator; the data trustee would be the data manager; and the end users who provide the corporation with their data would be the data beneficiaries.

restrict[ed] the access of Microsoft Germany to the information in its cloud" through legal and technological means.[39]

In the United States, however, similar contractual relationships would not yield the same results.[40] For example, it is under an insurance contract that we grant confidential healthcare information to insurance providers. Insurers are under a contractual duty to keep this information secure. The Supreme Court of Mississippi, however, found that such insurance contracts do *not* create fiduciary duties and blamed the plaintiff, whose information was improperly disclosed, for placing "any special degree of trust or confidence" in the insurance company.[41] Furthermore, it is well accepted in the United States that the "mere presence of the term 'trust'" does not turn a contract into a trust and does not "transform the relationship between the parties . . . to that of a trustee and beneficiary."[42] A contract, then, cannot by

---

[39] Schwartz, *supra* note 37, at 1698 (describing how Microsoft's German data trustee, T-Systems, was independent from Microsoft and encrypted the data hosted on its cloud such that Microsoft could not access that data). Note, however, that in 2019, Microsoft stopped accepting new customers into this data arrangement. Due to an "evolution in customers' needs" and the structure's "limits" in addressing such shifting needs, new customers can access services that align with Microsoft's "global cloud offerings." Esat Dedezade, *Microsoft to Deliver Cloud Services from New Datacentres in Germany in 2019 to Meet Evolving Customer Needs*, MICROSOFT (Aug. 31, 2018), https://news.microsoft.com/Micros/2018/08/31/Microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs [https://perma.cc/WPB2-LYB4].

[40] *See, e.g.*, City Sols. v. Clear Channel Commc'ns, Inc., 201 F. Supp. 2d 1048, 1049 (N.D. Cal. 2002) ("It is a well-settled principle that parties to a contract do not by necessary implication become fiduciaries."). In fact, the court continues on to say that even in the context of requisite trust and confidence, contracts do not per se establish fiduciary duties. For example, "it makes great sense not to impose fiduciary duties concomitantly with confidentiality agreements. The existence of a detailed confidentiality agreement suggests arm's-length dealings between co-equals." *Id.* Nonetheless, some courts do hold that "[i]f a contract establishes a relationship of trust and confidence between the parties, . . . *then a fiduciary duty arises from the contract which is independent of the contractual obligation.*" Lumbermens Mut. Cas. Co. v. Franey Muha Alliant Ins. Servs., 388 F. Supp. 2d 292, 305 (S.D.N.Y. 2005) (emphasis added). This framing is misleading because it conflates two independent sources of law. While "fiduciary duties may arise out of a contractual relationship," it is the *relationship* established by the contract rather than the contract itself that generates fiduciary duties. *Id.*

[41] Robley v. Blue Cross/Blue Shield, 935 So. 2d 990, 995 (Miss. 2006) ("Although one does not typically enter into a contract with another person unless he or she has a degree of trust or confidence in that person, without more, such a transaction amounts to merely a business relationship and not a fiduciary relationship."). *But cf.* Lee Craig, *Why a First Party Insurer Is Not a Fiduciary*, BUTLER WEIHMULLER KATZ CRAIG LLP (Nov. 16, 1999), https://www.butler.legal/why-a-first-party-insurer-is-not-a-fiduciary [https://perma.cc/TBD4-KLUX] (noting that the Supreme Court of Nevada "opined" that the insurer-insured relationship is "'akin'" to a fiduciary one). In fact, Nevada's position on the matter has strengthened over time, evidenced by the removal of the words "akin to": "The insurer-insured relationship is fiduciary in nature." Ins. Co. of the W. v. Gibson Tile Co., 134 P.3d 698, 703 (Nev. 2006).

[42] *In re* Martin, 35 B.R. 982, 985 (Bankr. E.D. Pa. 1984) (citing Davis v. Aetna Acceptance Co., 293 U.S. 328, 334 (1934)); Davis v. Aetna Acceptance Co., 293 U.S. 328, 334 (1934) ("The resulting obligation is not turned into one arising from a trust because the parties to one of the

mere language create a trust; nor is a trust merely a contractual relationship.[43]

Unlike contracts, Anglo-American trusts are creatures of equity, with roots in the English courts of chancery (not English courts of law).[44] While the historical details may not be of relevance to this Essay, the following short explanation may help clarify the discussion below. To this day, trusts are relationships where interests in property are separated.[45] Equitable interests are granted to the beneficiary while the legal property interests are

documents have chosen to speak of it as a trust."); *In re* Long, 44 B.R. 300, 305 (Bankr. D. Minn. 1983) ("Mere use of the words 'trustee,' 'trust,' or 'express trust' does not alone create a fiduciary relationship . . . ."). Matter of Emporelli, 42 B.R. 814, 819 (Bankr. W.D. Pa. 1984) ("[I]t is well-settled that the mere presence of language in an agreement purporting to create a trust is not determinative for purposes of nondischargeability."). *In re* Long, 44 B.R. at 305 ("The court will look not only at the language, but at the relationship and acts of the parties to determine whether a trust exists."); *In re* Schnitz, 52 B.R. 951, 955 (W.D. Mo. 1985) ("It must be emphasized, however, that the mere presence of the term 'trust' in a contract 'is generally insufficient' . . . to create a trust . . . ."). *See also* City of Hope Nat'l Med. Ctr. v. Genentech, Inc., 181 P.3d 142, 152 (Cal. 2008) ("[O]ne [contractual] party's ability to exploit a disparity of bargaining power between the parties does not necessarily create a fiduciary relationship." (citations omitted)).

43 Stinnett v. Colo. Interstate Gas Co., 227 F.3d 247, 253 (5th Cir. 2000) (noting that Texas law "eschews a rule of contract-based fiduciary duty, holding instead that such a duty 'arises from the relationship and not from express or implied terms of the contract or deed'" (quoting Manges v. Guerra, 673 S.W.2d 180, 183 (Tex. 1984))); AMY MORRIS HESS, GEORGE GLEASON BOGERT & GEORGE TAYLOR BOGERT, BOGERT'S THE LAW OF TRUSTS AND TRUSTEES § 17, Westlaw (database updated June 2022) ("[A] trust which is completely created needs no consideration to support it and make it enforceable . . . Contracts are still dependent on consideration for their enforceability. This is a marked distinction between a trust and a contract."); *In re* Naarden Tr., 990 P.2d 1085, 1089 (Ariz. Ct. App. 1999) ("[T]he undertaking between the settlor and trustee is not properly characterized as contractual . . . ."); Gibbons v. Anderson, 575 S.W.3d 144, 148 (Ark. Ct. App. 2019) ("[A] trust agreement is not a contract."); *In re* Calomiris, 894 A.2d 408, 410 (D.C. 2006) ("[A]n inter vivos trust is not a contract." (internal quotation marks omitted) (quoting Schoneberger v. Oelze, 96 P.3d 1078, 1079 (Ariz. Ct. App. 2004))); *In re* Will of Allis, 94 N.W.2d 226, 229 (1959) ("[A] testamentary trust is not a contract."). *See also* UNIF. TR. CODE § 105 cmt. (UNIF. L. COMM'N 2000) (clarifying that even the "terms of a [written express] trust may not deny a court authority to take such action as necessary in the interests of justice").

44 *See generally* John H. Langbein, *The Contractarian Basis of the Law of Trusts*, 105 YALE L.J. 625 (1995). Note also that although the substantive distinction between law and equity has been all but erased in the minds of many judges, legislators, legal academics, and even law students, equity still "hangs on by its fingernails," refusing to be fully incorporated into law. Henry E. Smith, *Equity as Meta-Law*, 130 YALE L.J. 1050, 1054–59 (2021); *see also* Samuel L. Bray, *The Supreme Court and the New Equity*, 68 VAND. L. REV. 997, 1053 (2015) ("[The Supreme] Court is acting directly contrary to the conventional wisdom in remedies scholarship over the last four decades [that law and equity are completely merged]. In these cases, the Court has preserved the line between legal and equitable remedies.").

45 *See* RESTATEMENT (THIRD) OF TRUSTS § 2 (AM. L. INST. 2003) (noting that a trust "is a fiduciary relationship with respect to property" where "the person who holds title to the property" has "duties to deal with it for the benefit of charity or for one or more persons, at least one of whom is not the sole trustee"); *id.* § 3 (stating that "[t]he person who creates a trust is the settlor"; "[t]he property held in trust is the trust property"; "[t]he person who holds property in trust is the trustee"; and "[a] person for whose benefit property is held in trust is a beneficiary").

held by the trustee.[46] Once a trust is established,[47] it is the trustee who owns legal title to the asset; the trustee has an in rem right, a right good against the world.[48] It is the trustee who imposes the "world's duty not to trespass" or otherwise interfere with the property.[49] The beneficiary, on the other hand, is granted the beneficial interest in the property. This is an equitable interest granting "rights in personam against the holder of the legal title," the trustee.[50]

Now, with a shared understanding of trusts, yet another distinction is equally relevant. The distinction is between rights subject to the law of contracts and those that are governed by the law of property.[51] It is uncontroversial to say that data can be the subject of contract,[52] but because trusts and their fiduciary duties cannot be created by contract, this mere fact is not helpful in validating the viability of data trusts.[53] The important question is whether data falls into the category of "property" for the purposes of existing trust law in the United States. This crucial question, though, is not always made explicit when the proponents of data trusts describe their projects and policy goals, leaving such critical legal hurdles to mere parentheticals and footnotes.[54] If trusts and their fiduciary duties require *trust property*, and if data cannot be such *trust property*, the very purposes of

---

46 The trustee's interest may also be equitable, but diving into the many possible arrangements of American trusts beyond what is explored below will not further the arguments of this Essay. *See* RESTATEMENT (THIRD) OF TRUSTS § 2 cmt. d (AM. L. INST. 2003) ("Although trust beneficiaries have equitable title, a trustee's title to trust property may be either legal or equitable. Although it is usually true . . . that the trustee has legal title . . . .").

47 For our purposes, it suffices to say that trusts may be established by written or spoken words and by the "interpretation of the words or conduct of the settlor in the light of all of the circumstances surrounding the creation of the trust." RESTATEMENT (THIRD) OF TRUSTS § 4 cmt. a (AM. L. INST. 2003) (explaining possible sources of the "terms of the trust").

48 *See, e.g.*, Thomas W. Joo, *Contract, Property, and the Role of Metaphor in Corporations Law*, 35 U.C. DAVIS L. REV. 779, 809 (2002) (discussing property rights in general and distinguishing them from contract rights).

49 *Id.* at 809–10 (explaining how property law defines a property right by giving third parties duties to the holder of the property right).

50 Comm'r v. Nevius, 76 F.2d 109, 110 (2d Cir. 1935) (distinguishing property law's regime of legal and equitable interests held in trust from the tax code's treatment of such assets, the latter of which focuses solely on which interests happen to have "pecuniary value").

51 For a fuller theoretical inquiry into this distinction, see Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 851–52 (2001) ("The difference corresponds to the distinction between in rem rights and in personam rights . . . . [T]he distinction . . . 'is absolutely vital to grasping legally recognized practices like property' . . . ." (quoting J.E. PENNER, THE IDEA OF PROPERTY IN LAW 30 (1997))).

52 *See, e.g.*, Ned T. Himmelrich, *A New Breed of Copyright Issues*, MD. BAR J., Nov.–Dec. 2003, at 18, 21 (noting that licenses are used to protect and manage data "through contract terms").

53 *See* Joo, *supra* note 48, at 809–10 (explaining that contract law could not simulate property rights because "transaction costs would be too great").

54 *See, e.g.*, MOZILLA INSIGHTS ET AL., *supra* note 33, at 14 ("[S]ignificant questions remain about which laws are compatible where (for either 'data' or 'rights to data') . . . ."; Digit. Civ. Soc'y Lab, *supra* note 33 (investigating the use of "data trusts within the context of civil society organizations").

fiduciary duties in this context—to protect data privacy or autonomy, or to promote any other goal of data governance—will be left unfulfilled.

II
DATA RIGHTS AND THE TRUST PROPERTY

For the purposes of trust law, "property" refers to "interests in things, not necessarily the things themselves, but necessarily things that are legally capable of being owned . . . and to which property interests can attach."[55] This definition has been applied quite liberally to include real and personal property as well as tangible and intangible property.[56] It may even include intellectual property rights, shares of a company, or a beneficiary's interest in a life insurance policy.[57] Thus, trust property—the trust *res*—is not limited to tangible chattel or even to in rem property interests. As broad as this definition is,[58] however, data (or data rights) may nonetheless fail to meet it, as the discussion below demonstrates.

If trust property must refer to "things that are legally capable of being owned,"[59] the key question for the creation of data trusts, then, is whether data can be *owned*. From the way we discuss data colloquially, it may seem that the answer is an unquestionable yes. I talk about "my data" or the company's data. But legally, the answer is far from clear. Scholars, judges, and legislators are still struggling to determine whether or how data can be owned, what such ownership would mean, and what body of law would govern such ownership.[60] While a few cases have already treated nonrival[61] electronic documents and data as property for the narrow purposes of conversion claims, there is still significant disagreement among courts.[62]

---

55 RESTATEMENT (THIRD) OF TRUSTS § 40 cmt. b (AM. L. INST. 2003).

56 *See id.* (describing the diverse set of rights that trust property may encompass); Jeremiah Lau, James Penner & Benjamin Wong, *The Basics of Private and Public Data Trusts*, 2020 SING. J. LEGAL STUD. 90, 103 (2020) ("[T]he law of trusts tends to be fairly liberal about the kind of assets that can be held on trust.").

57 RESTATEMENT (THIRD) OF TRUSTS § 40 cmt. b (AM. L. INST. 2003).

58 *See* Lau, Penner & Wong, *supra* note 56.

59 RESTATEMENT (THIRD) OF TRUSTS § 40 cmt. b (AM. L. INST. 2003).

60 For a non-exhaustive list of competing judicial and academic analyses, see João Marinotti, *Tangibility as Technology*, 37 GA. ST. U. L. REV. 671, 723 n.239 (2021).

61 *See id.* at 697 (defining nonrival goods in this context as those, such as "intellectual property, information, or data," that can be copied perfectly and taken or used by person *B* such that the original owner *A* suffers no deprivation of use or access); *see also* Thomas C. Brown, John C. Bergstrom & John B. Loomis, *Defining, Valuing, and Providing Ecosystem Goods and Services*, 47 NAT. RES. J. 329, 357 (2007) ("A *rival* good is one for which consumption by one person reduces the amount of good or service available to others, as is the case with apples and haircuts.").

62 *See, e.g.*, Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1278 (N.Y. 2007) ("[E]lectronic documents and records stored on a computer can also be converted . . . ."); Integrated Direct Mktg., LLC v. May, 495 S.W.3d 73, 76 (Ark. 2016) ("[E]lectronic data . . . can be converted if the actions of the defendant are in denial of or inconsistent with the rights of the owner or person entitled to possession."). *But see, e.g.*, Epic Sys. Corp. v. Tata Consultancy Servs. Ltd., No. 14-

Given this lack of legislative, precedential, and academic support, some commentators go so far as to say that data is not ownable at all under any body of existing American law.[63] With this background in mind, proponents of data trusts attempt to bypass this controversial topic by arguing that a common law legal property interest is not necessary for the creation of a trust. As explained below, they go on to argue that data rights as created by privacy or consumer protection statutes are sufficient to be placed in trust as a trust *res* without solving the thorny question of data propertyhood.[64] The following discussion demonstrates that such an approach runs with equal force into various dead or perplexing ends, making the discussion of data propertyhood a necessity yet again.

While European data trusts are outside the scope of this Essay, commentators sometimes argue that the *rights* granted under Europe's General Data Protection Regulation (GDPR)—and, similarly, the California Consumer Privacy Act (CCPA)[65] or the Illinois Biometric Information Privacy Act (BIPA)[66] in the United States[67]—may themselves be placed into data trusts as trust property.[68] Such arguments, however, fail to prove that

CV-748, 2016 WL 4033276, at *27 (W.D. Wis. July 26, 2016) ("[T]here is, at least so far, no support from Wisconsin courts for such an expansion of this state's common law [to recognize conversion claims of electronic data] . . . ."); Wells v. Chattanooga Bakery, Inc., 448 S.W.3d 381, 392 (Tenn. Ct. App. 2014) ("[A]n action for the conversion of intangible personal property is not recognized in Tennessee.").

63 *See, e.g.*, Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 42–43 (2018) ("Existing property laws intentionally *exclude* data from subject matter definitions."); Sylvia Zhang, *Who Owns the Data Generated by Your Smart Car?*, 32 HARV. J.L. & TECH. 299, 305 (2018) ("Raw data cannot be 'owned' in the same legal sense that traditional intellectual property can be owned . . . .").

64 *See infra* notes 65–70 and accompanying text.

65 *See generally* MICHAEL BAHAR & MARY JANE WILSON-BILIK, EVERSHEDS SUTHERLAND, CALIFORNIA'S NEW DATA PRIVACY LAW: WHAT YOU NEED TO KNOW (2018), https://us.eversheds-sutherland.com/portalresource/lookup/poid/Z1tOl9NPluKPtDNIqLMRV56Pab6TfzcRXncKbDtR r9tObDdEpSpDm83!/fileUpload.name=/Cali%20new%20data%20privacy%20law.pdf [https://perma.cc/TGB5-TC4P] (explaining the CCPA's jurisdictional reach and the new rights over personal data created by the Act). For updates to the CCPA, see Webb McArthur, *California Governor Approves Changes to CCPA and CPRA*, AM. BAR ASS'N: BUS. L. TODAY (2021), https://businesslawtoday.org/month-in-brief/october-in-brief-business-regulation-and-regulated-industries-2021 [https://perma.cc/JWF7-9KP5].

66 740 ILL. COMP. STAT. ANN. 14/1 (West 2008); *see also* Lauren Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C. L. REV. 349, 370 (2018) (describing Illinois's "comprehensive law addressing businesses' collection and use of biometric information").

67 *See* Geoffrey Xiao, *Bad Bots: Regulating the Scraping of Public Personal Information*, 34 HARV. J.L. & TECH. 701, 715 (2021) (noting how both California's CCPA and Illinois's BIPA grant residents of those states a set of rights similar to, though not exactly the same as, the GDPR in Europe).

68 *See, e.g.*, Sylvie Delacroix & Neil D. Lawrence, *Bottom-up Data Trusts: Disturbing the*

the data rights under the GDPR are sufficiently akin to property rights for the purposes of trust law, rather than being akin to the rights of bodily autonomy or privacy,[69] which are inalienable and cannot be placed in a trust.[70] Furthermore, as Professor Kieron O'Hara has noted, the GDPR-centric data trust model fails to solve an underlying power asymmetry that it was originally meant to solve because it "assumes that the data subject is *unable* to give informed consent to a data controller . . . but at the same time is *able* to understand and initiate legal relations with the trustee."[71] In other words, how would consumers have the legal sophistication and positional power to understand and tailor their relationship with a data trustee beyond their (in)ability to understand and negotiate existing big tech terms of service? They likely wouldn't.

Thus, if GDPR-like rights (e.g., rights granted under the CCPA or BIPA) are not sufficient to establish a recognizable trust *res*, we must return to the hotly debated legal status of data under American property law to then determine if data can serve as a trust *res*. And, as noted above, the caselaw on the subject has not brought us closer to a consensus, nor have analyses of public policy or legal theory. On one side of the debate, Professors Paul Schwartz and Lawrence Lessig have offered accounts of how data ownership through property law could usher in an era of responsible governance through a commodified data market in which data owners would be able to control the use of their personal information.[72] On the other side, Professors

'One Size Fits All' Approach to Data Governance, 9 INT'L DATA PRIV. L. 236, 236 (2019) ("[T]he data trustees would exercise the *data rights conferred by the GDPR* (or other top-down regulation) on behalf of the Trust's beneficiaries.") (emphasis added). *But see, e.g.*, Wendy Jing Wen Xu, *Recognizing Property Rights in Biometric Data Under the Right of Publicity*, 98 U. DET. MERCY L. REV. 143, 161 n.161 (2020) (noting that BIPA and other "biometric data legislative schemes deal exclusively with privacy rights, not property rights"); Greg Lastowka, *User-Generated Content and Virtual Worlds*, 10 VAND. J. ENT. & TECH. L. 893, 896 (2008) (noting that if individuals "have any right to object to the monetization of [their] data, it is via a right of privacy, not property").

69 Some commentators go so far as to say that "when people argue for 'property over data,' they are arguing for 'some kind of right over data, not necessarily a property right, that is protected by a property rule.'" Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. 501, 571 (2021) (going on to argue that data property is "inadequate at protecting privacy rights" because "[d]ata property proposals leave out important dignitary considerations, ignore asymmetric information and unequal bargaining power, and fail to address the harms produced by aggregated and inferred personal data").

70 *See* RESTATEMENT (THIRD) OF TRUSTS § 40 cmt. d (AM. L. INST. 2003) ("[A] personal injury cause of action is not transferable and cannot thereby be made the subject of a trust." (quoting Vittands v. Sudduth, 730 N.E.2d 325, 333 (Mass. App. Ct. 2000))).

71 Kieron O'Hara, *Data Trusts*, 6 EUR. DATA PROT. L. REV. 484, 489, 491 (2020) ("[L]iteral data trusts aren't going to solve the Facebook problem, and neither will metaphorical data trusts work as PR exercises for the tech giants.").

72 *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2125–26 (2004) ("A strong conception of personal data as a commodity is emerging . . . . This Article's goal has been to develop a model for the propertization of personal information that also

Pamela Samuelson, Mary Fan, and Dan Hunter have variously argued that a market over property rights in data would not only hinder efforts at protecting individual privacy and security, but would also create a cyber anticommons, hindering innovation and economic activity writ large.[73]

The sheer number of competing viewpoints demonstrates that defining the exact nature of property (or non-property) rights to data will require significant attention before any consensus can be reached.

A. Trust Law and the Res

Despite these disagreements over the exact legal nature of data, trust law may be able to bypass such questions entirely. Note that ownership over a trust *res* may refer to ownership over land, chattel, choses in action, life insurance, good-will, trademark, trade secrets, intellectual property, stocks, bonds, and even beneficial interests in other trusts.[74] In summary, property of many forms may be held in trust.[75] What is important is not the exact nature of each type of property capable of being held in trust, but rather what they all have in common. Determining the legal nature of data may not be required if we can determine that data shares these common features and is,

---

exhibits sufficient sensitivity to attendant threats to personal privacy."); *id.* at 2094 ("[T]he understanding of property as a bundle of interests . . . helps frame a viable system of rights with respect to personal data . . . [focusing on]: inalienabilities, defaults, a right of exit, damages, and institutions."); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63 (1999) (noting that those who use individuals' data could be forced to internalize the cost of doing so via property laws which would enable those individuals to engage in market negotiation).

73 *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1129 (2000) ("A property rights model for protecting personal data nevertheless presents many problems."); *see also* Mary D. Fan, *Private Data, Public Safety: A Bounded Access Model of Disclosure*, 94 N.C. L. REV. 161, 205–06 (2015) ("Data ownership and control has the power to illuminate or obscure dangers to public health and safety."); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 518–19 (2003) (noting that commercial businesses have "now . . . convince[ed] judges to carve out remarkable new property rights online . . . [and] eroded cyberspace's public commons, [which] . . . threaten[s] to create a genuine digital anticommons."). Anticommons property may emerge when "multiple people hold rights of exclusion to a property such that no one has an effective right of use." Hunter, *supra*, at 444. As a result, the property may be "locked into suboptimal and wasteful uses because the holders of the exclusion rights block the best use of the resource"—a "tragedy of the anticommons." *Id.* As another example of the negative consequences of creating a market for property rights in data, Professor Samuelson notes that "[c]reating a property right in personal data may . . . be objectionable to those who consider information privacy to be a fundamental civil right." Samuelson, *supra*, at 1142.

74 *See generally* RESTATEMENT (THIRD) OF TRUSTS § 40 cmt. b (AM. L. INST. 2003) ("Trust property may be real or personal, tangible or intangible. It may consist of such diverse rights as undivided interests, terms of years, contingent future interests, and *choses in action* . . . . ").

75 But both the First and Second Restatements of the Law of Trusts note that "there are interests which are not property, such as the interest in freedom from harmful bodily contact or other interests in personality" which cannot "be made the subject of a trust." RESTATEMENT (FIRST) OF TRUSTS § 74 cmt. b (AM. L. INST. 1935); RESTATEMENT (SECOND) OF TRUSTS § 74 cmt. b (AM. L. INST. 1959) (same).

therefore, sufficiently "property-like" for the purposes of trust law.[76]

For data to be an eligible trust *res*, all that is necessary is a "definite or ascertainable" right to data whose immediate ownership can be easily discerned.[77] This requirement serves two purposes. First, it ensures that the contents and boundaries of the trust *res*—over which the trustees normally have a full unencumbered title such as fee simple absolute—are understood by all relevant parties.[78] As Professors Thomas Merrill and Henry Smith summarized:

> This permits the trustee to deal with [trust] assets the way a full owner would—by buying, selling, leasing, or mortgaging the assets as market conditions dictate, in order to maximize the risk-appropriate return to the trust. The beneficial interest, however, is often carved up among several beneficiaries spread over multiple generations. . . . If contingent remainders and executory interests were commonly encountered as in rem rights, they would greatly complicate the process of processing information about these rights, certainly for transactional and secured-lending purposes.[79]

Second, requiring a definite and ascertainable trust *res* serves an evidentiary purpose, ensuring that a trust can be unequivocally created through the unambiguous transfer and delivery of the trust *res*. It allows "the court to be confident that the settlor did indeed transfer the property to a

---

[76] That is not to say that the nuances of trust law are exactly the same across various American jurisdictions. As the Fifth Circuit explains in *Casa Orlando Apartments, Ltd. v. Fed. Nat'l Mortgage Ass'n*, 624 F.3d 185, 194 (5th Cir. 2010), "[w]hile the basic principles of fiduciary law may be the same throughout the country, the nuances vary, and those nuances affect the outcome of claims." The Fifth Circuit then catalogs differences among the factors necessary for the creation of a trust under the laws of several states; for example:

> In Illinois, for example, a valid express trust requires: 1) intent of the parties to create a trust as shown by a writing or by circumstances; 2) a definite subject matter of trust property; 3) ascertainable beneficiaries; 4) a trustee; 5) specifications of a trust purpose and how the trust is to be performed; and 6) delivery of the trust property to the trustee. . . . Under Texas law, a 'fiduciary relationship is an extraordinary one and will not be lightly created.' Thus, ordinarily 'an express trust does not arise unless the owner of property has shown an unequivocal intention to create a trust.' If 'the person to whom the settlor's wish is addressed has a clear discretion to act as he thinks fit,' no trust is created. . . . The District of Columbia has a simpler standard, requiring that 'the settlor need only manifest an intention to impose upon herself or upon a transferee of the property equitable duties to deal with the property for the benefit of another person.' The law of the District of Columbia further requires the trustee to take title of the trust assets. *Id.* at 194–95.

[77] RESTATEMENT (THIRD) OF TRUSTS § 40 cmt. e (AM. L. INST. 2003) ("There is no trust property if the identity of the intended subject matter remains wholly in the control of the settlor or if its description is so indefinite that it cannot be ascertained.").

[78] Fee simple absolute is the "broadest property interest allowed by law, [which] endures until the current holder dies without heirs." *Fee Simple*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[79] THOMAS W. MERRILL & HENRY E. SMITH, PROPERTY: PRINCIPLES AND POLICIES 771–72 (3d ed. 2017).

trustee for the benefit of the beneficiaries."[80] This certainty protects both the supposed settlor and the supposed trustee(s). Courts "protect the purported transferor . . . against false or mistaken claims that he or she had transferred the property away in a trust."[81] And given the "extraordinary" nature of fiduciary duties,[82] courts protect the purported trustee from being unwillingly subjected to the duties of prudence, loyalty, and impartiality, among others, for the benefit of the settlor.[83]

In this requirement, there is a doctrinal focus on factual clarity rather than on the legal nature of the assets held in trust. Knowledge and certainty (e.g., about what constitutes the trust *res*) are significantly more crucial for the purposes of trust law than a formalistic analysis of the legal nature of the underlying trust corpus. This factual focus has allowed trusts to evolve from tools largely meant to manage "land, personal property, and intellectual property rights" to tools used to govern "stocks, bonds, and other readily-marketable intangible assets with income-earning potential."[84] As the contents of the trust corpus have become more and more abstract, the need for defined rights and clear delivery has only grown stronger. Clarity in the ownership structure of trusts is now crucial not only in protecting settlors but also in "promot[ing] the reliance of outsiders, such as lenders and other creditors."[85]

Given data's prominence as a market-ready, income-earning asset, the desire to create, manage, and profit from data trusts is not surprising. Data, after all, has been called the "'oil' of the modern economy."[86] A crucial question, therefore, is whether data can fulfill the factual clarity required of a trust *res*. Are data or data rights sufficiently defined? Can the delivery of data be unambiguously ascertained? These questions have not been sufficiently addressed for data trusts to be accepted as legitimate creations of

---

80 John H. Langbein, *Mandatory Rules in the Law of Trusts*, 98 NW. U. L. REV. 1105, 1121 (2004).

81 *Id.*

82 Stinnett v. Colo. Interstate Gas Co., 227 F.3d 247, 253 (5th Cir. 2000) (noting that "[a] fiduciary relationship is an extraordinary one and will not be lightly created" since "[f]iduciary duties do not abound in every, or even most, garden variety, arms-length contractual relationships, even those among trusting friends" (first citing Castillo v. First City Bancorporation of Tex., 43 F.3d 953, 957 (5th Cir. 1994); and then citing Crim Truck & Tractor Co. v. Navistar Int'l Transp. Corp., 823 S.W.2d 591, 594–95 (Tex. 1994))).

83 *See* RESTATEMENT (THIRD) OF TRUSTS pt. 6, ch. 15, intro. note (AM. L. INST. 2003) ("The core of trust fiduciary law is . . . the trustee's duties of *prudence* . . . , *loyalty* . . . , and *impartiality* . . . ."); *id.* § 35 cmt. a ("Given the nature of the fiduciary relationship, it is inappropriate to force a person to act in that capacity.").

84 MERRILL & SMITH, *supra* note 79, at 770.

85 Langbein, *supra* note 80, at 1121.

86 *See, e.g.*, Matthew S. DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2451 (2018) ("This constant flow of information, and the insights and revenues it can generate for businesses, has led to data being described as the 'oil' of the modern economy. Recognizing this potential, businesses have for years identified their data stores as among their most prized assets.").

private law. One reason for this is that data may have multiple independent, overlapping, or even contradictory definitions, undermining trust law's requirement of a definite and ascertainable trust *res*.

B. Defining Data (Rights)

In the confines of this Essay, I do not aim to provide an exhaustive list of the ways in which the word "data" is currently used; a comprehensive taxonomy of digital information assets could surely encompass an entire book, if not more. Nonetheless, the purpose of this Section is to demonstrate that cleanly and clearly defining data rights such that they are sufficiently definite and ascertainable for the purposes of trust law—or choosing one of many potential definitions—will be a difficult task. It will be especially difficult to define through a common law process, as would necessarily be the case without legislative intervention.

Generically, "data" can simply mean "factual information."[87] This definition encompasses everything ranging from Napoleon Bonaparte's height[88] to the current temperature in your house. But as Professor Ignacio Cofone has noted, "[n]either under existing law nor under data property would I have a right, for example, to prevent other people from noticing I bought a banana when I went to the supermarket."[89] At most, I would retain a right to prevent the store owner from entering "the information into a customer data bank to then sell to third parties."[90] Thus, as may have been expected, mere information (i.e., facts) is not a sufficiently narrow definition of data for ownership purposes.

More narrow definitions have been statutorily created in the context of personally sensitive information. But even within relatively comparable frameworks, definitions contain significant differences that would alter the rights held under data ownership. Take the CCPA and GDPR's definitions of "personal information" and "personal data," respectively, as listed in Table 1.

TABLE 1

CCPA	*Personal information* is information that identifies, relates to, or could reasonably be linked with *you or your household.*[91]

87 *Data*, *supra* note 1.

88 *See* Una McIlvenna, *Was Napoleon Short? Origins of the 'Napoleon Complex,'* HISTORY (Nov. 13, 2019), https://www.history.com/news/napoleon-complex-short [https://perma.cc/Y5XH-33E6] ("Napoleon's height was just over '*5 pieds 2 pouces*' (5'2"). Applying the French measurements of the time, that equals around 1.69 meters, or just over 5'5". So at 5'5" he was just an inch or so below the period's average adult male height.").

89 Cofone, *supra* note 69, at 521.

90 *Id.* (engaging in a hypothetical thought experiment).

91 CAL. CIV. CODE § 1798.140(o)(1)(A)–(K) (West 2022) (emphasis added).

GDPR	*Personal data* means any information *relating to* an identified or identifiable *natural person* ("data subject").[92]

While these definitions may appear superficially similar, there is a subtle but significant difference. Unlike the GDPR's definition of "personal data," the CCPA's "definition of personal information specifically includes *household information*."[93] Thus, the underlying data pool considered to be personal information under the CCPA is, in some respects, a lot broader than under the GDPR.[94] That said, the CCPA, "apart from allowing individuals to opt out of sales of their personal data, affords individuals little control" over, for example, the initial collection of such data.[95] The GDPR, on the other hand, attempts to "enable individuals to refuse to give companies their data in the first place."[96] And as Anupam Chander, Margot Kaminski, and William McGeveran have noted, unlike the CCPA, the GDPR grants individuals "robust rights throughout the life cycle of data processing, including the right to rectification of incorrect information; the right to prevent automated individual decision-making and to receive explanation of any automated decision; and broader rights related to erasure of data and withdrawal of consent."[97]

Without legislative intervention, which version of "personal information" would a data trust rely on? Would household information qualify? Which set of individual rights would a data trustee manage on behalf of the data generators? One could imagine that such necessary details could be defined in the trust document itself. Such details, however, are not usually left to the discretion of the private parties involved in the trust's creation; they are predefined by law, as the following analogy illustrates.

Instead of data, imagine a trust created to manage a plot of land. As is expected, the land "can be bought and sold, invested and reinvested, leased and mortgaged, in the sound discretion of the trustee as if the property were an undivided fee simple."[98] The trustee's power to manage in this way relies

92 Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 3 (emphasis added), https://data.europa.eu/eli/reg/2016/679/2016-05-04 [https://perma.cc/F7RB-HDGN].

93 Carol A.F. Umhoefer, *CCPA vs. GDPR: The Same, Only Different*, DLA PIPER (Apr. 11, 2019) (emphasis added), https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr [https://perma.cc/FW4R-TGDD].

94 *See generally GDPR/CCPA High-Level Comparison Chart*, PERKINS COIE, https://www.perkinscoie.com/images/content/2/0/v4/204145/2108-CCPA-Comparison-Chart-v.3.pdf [https://perma.cc/57BR-93A2].

95 Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1757 (2021).

96 *Id.*

97 *Id.* at 1757–58.

98 Merrill & Smith, *supra* note 51, at 849.

on the fact that "the trust entails the transfer of *full legal title* over assets to the trustee . . . [so] the trustee exercises most of the *bundle of in rem rights* associated with these assets."[99] The trust does not and cannot define the bundle of in rem rights associated with the underlying asset; that is a matter of property law.[100]

As Thomas Merrill and Henry Smith have explained, trust law's reliance on legally defined rights (i.e., rights defined by law) over the underlying asset is no accident. If the in rem rights associated with the trust asset were able to be defined by the trust instrument itself, new types of in rem property rights would be created by individuals as needed.[101] A consequence of this open-ended list of property rights would be that third parties would "incur additional costs of gathering information in order to avoid violating novel property rights or to decide whether to seek to acquire these rights."[102]

Third parties engaging with the trustee would have to become intimately familiar with the terms of the trust (if they even know that a trust exists) in order to determine whether the trustee is legally allowed to engage in any potential third-party transaction involving the underlying trust asset.[103] This would undermine one of the purposes of trust law;[104] it would compromise "the reliance of [third parties], such as lenders and other creditors," on the legal legitimacy of a trustee's management decisions.[105] Because trust law grants the trustee rights defined by law (not by individuals), third parties need not consider the details of the trust when engaging with the trustee. Rather, "when issues arise that implicate the in rem rights associated with the trust assets, the fact that the assets are held in

---

99 *Id.* at 847 (emphasis added).

100 Specifically, the property law principle of numerus clausus (which is implicit in common law systems) "prevents the customization of property interests. In the absence of this simple common law rule, the normative commitments that comprise our rights and duties with respect to the tangible objects in the world would rapidly grow so complex as to overwhelm our capacity to understand them, let alone enforce them." Meredith M. Render, *Complexity in Property*, 81 TENN. L. REV. 79, 82 (2013); *see also* Christina Mulligan, *A Numerus Clausus Principle for Intellectual Property*, 80 TENN. L. REV. 235, 238 (2013) ("Contracts are generally governed by default rules that can be freely altered . . . . In contrast, a transfer of real or tangible property is forbidden unless the transfer is . . . within one of 'a limited number of standardized forms.'").

101 Although "the relations among *parties to a trust agreement* [i.e., the settlor, trustee, and beneficiary] are governed by legal rules that track the law of *contract*," which can generally be tailored by the contracting parties, the legal property interests held by the trustee are "limited to a small number of standardized types." Merrill & Smith, *supra* note 51, at 796, 845 (emphasis added).

102 *Id.* at 777 ("[F]ree customization of property forms would create an information-cost externality; mandatory standardization is the legal system's way of reducing these external costs to an acceptable level.").

103 *See id.*

104 *Id.* at 849 ("In effect, the trust is a brilliant device that allows for considerable customization of beneficial interests . . . while at the same time consolidating the assets used to fund these beneficial interests in a form that *minimizes third-party information costs*.") (emphasis added).

105 Langbein, *supra* note 80, at 1121.

trust is generally irrelevant to the resolution of these issues."[106] Ultimately, the reliance on legally defined rights allows trust law to lower information costs and increase efficiency.[107]

By applying this analogy and analysis to trusts over data, it becomes apparent that the law of trusts cannot leave the definition and scope of data rights to the discretion of individuals (e.g., settlors). The definitions must be defined by law. Without legislative intervention, then, the definition and scope of data for the purposes of data trusts, and the scope of rights granted to trustees would be up to the courts. Unlike in the context of contract interpretation, however, the definitions and rights acknowledged by courts would not be limited to each individual trust. Such definitions and rights, much like the in rem rights over land,[108] would be applied to all data trusts.

A uniform set of definitions and rights over data established by courts may seem useful until courts attempt to apply these same rights, rules, and restrictions to data of various types. Given the variation in data governance regimes, it seems evident that various different rules should apply to the various different categories and definitions of data. For example, within the Environmental Protection Agency (EPA), there are distinct rules for Personally Identifiable Information (PII); Sensitive Personally Identifiable Information (SPII); Proprietary Business Information (PBI); Unclassified Controlled Technical Information (UCTI); Sensitive but Unclassified (SBU); For Official Use Only (FOUO); Law Enforcement Sensitive (LES); and other types of data.[109] Health data governed by the Health Insurance Portability and Accountability Act (HIPAA),[110] too, is not all treated equally;[111] the HIPAA Privacy Rule applies to "individually identifiable health information, called protected health information," while the HIPAA Security Rule applies only to "individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form," which it labels "'electronic protected health information' (e-PHI)."[112]

Given the diverse nature of the underlying data in question, it is no

---

106 Merrill & Smith, *supra* note 51, at 847.

107 *Id.* at 840, 849 (noting also how similar arrangements of in rem and in personam rights decrease information costs and increase efficiency in the law of security interests).

108 *See, e.g.*, JOHN A. BORRON, JR. & LEWIS M. SIMES, SIMES AND SMITH: THE LAW OF FUTURE INTERESTS § 62 THE POSSESSORY ESTATES (3d ed. 2002) (defining "fee simple, the fee tail, . . . the life estate, the term of years, the periodic tenancy, and the tenancy at will").

109 *Controlled Unclassified Information (CUI) Program Frequently Asked Questions (FAQs)*, ENV'T PROT. AGENCY, https://www.epa.gov/cui/controlled-unclassified-information-cui-program-frequently-asked-questions-faqs [https://perma.cc/A5F5-HUMJ].

110 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

111 *See Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html [https://perma.cc/U4D8-A5F4].

112 *Id.* ("The Security Rule does not apply to PHI transmitted orally or in writing.").

wonder that each of these data governance regimes defines data and data rights differently. A single set of definitions and rights would likely fail to achieve the normative goals of data rights, data privacy, and data protection regimes.

C. Beyond Information

So far, this Part has discussed the wide variety of personal or otherwise sensitive information that has been subject to data governance regimes or to proposed data property rights. Yet this is not where the discussion of data ownership ends. Databases, individual digital files, and stored emails, among other digital assets, have also raised questions of data ownership.

For an illustrative example regarding emails and files, let us turn to the case of Louis Thyroff.[113] Louis was an insurance agent for the Nationwide Mutual Insurance Company (Nationwide) who was leased a work computer in 1988. This allowed Louis to more easily access, use, edit, and add customer information to Nationwide's centralized computers. It also granted him the ability to check his personal emails and to store his personal documents on the computer's hard drive.

Unfortunately, twelve years later, Louis was terminated, and the company repossessed his computer and denied him further access to its electronic records and data. As the New York Court of Appeals noted (when answering a certified question from the Second Circuit Court of Appeals), Louis was "unable to retrieve his customer information and other personal information that was stored on the [Nationwide] computers."[114]

Louis sued Nationwide for, among other claims, the conversion of his electronic documents.[115] In determining whether the tort of conversion applied to intangible electronic files such as those on Louis's hard drive, the New York Court of Appeals concluded that

> electronic documents and records stored on a computer can . . . be converted by simply pressing the delete button . . . . [I]t generally is not the physical nature of a document that determines its worth, it is the information memorialized in the document that has intrinsic value. A manuscript of a novel has the same value whether it is saved in a computer's memory or printed on paper. So too, the information that Thyroff allegedly stored on his leased computers in the form of electronic records of customer contacts and related data has value to him regardless of whether the format in which the information was stored was tangible

---

113 Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272 (N.Y. 2007); *see also, e.g.*, Thompson v. UBS Fin. Servs., Inc., 115 A.3d 125, 132 (Md. 2015) (noting that "digital media is capable of being converted" while maintaining the validity of the merger doctrine). *But cf.* Wells v. Chattanooga Bakery, Inc., 448 S.W.3d 381, 392 (Tenn. Ct. App. 2014) ("[A]n action for the conversion of intangible personal property is not recognized in Tennessee.").

114 *Thyroff*, 864 N.E.2d at 1273.

115 *Id.*

> or intangible. In the absence of a significant difference in the value of the information, the protections of the law should apply equally to both forms—physical and virtual.
>
> In light of these considerations, we believe that the tort of conversion must keep pace with the contemporary realities of widespread computer use. We therefore . . . hold that the type of data that Nationwide allegedly took possession of—electronic records that were stored on a computer and were indistinguishable from printed documents—is subject to a claim of conversion in New York. Because this is the only type of intangible property at issue in this case, we do not consider whether any of the myriad other forms of virtual information should be protected by the tort.[116]

While the court acknowledged that determining the status of property rights over the "myriad other forms of virtual information" would be difficult, if not impossible, it did grant Louis the property ownership over the data he lost. He was able to sue Nationwide for the conversion of his electronic documents. Note that the nature of these documents is vastly different from the types of information discussed above. Louis does not have ownership over each electronic document because it "identifies, relates to, or could reasonably be linked with" him.[117] Rather, in this particular case, the court employed a labor theory of property[118] to recognize Louis's rights in the lost documents. The court found that "virtual creation" was sufficiently like "production by pen on paper or quill on parchment" to yield similar property rights.[119]

Unfortunately for Louis, and despite this ruling from the New York Court of Appeals, the U.S. District Court for the Western District of New York granted Nationwide's motion for summary judgment, and the Second Circuit affirmed.[120] Even though New York law would recognize his claim

---

116 *Id.* at 1278.

117 CAL. CIV. CODE § 1798.140(o)(1)(A)–(K) (West 2022).

118 *See generally* Adam Mossoff, *Locke's Labor Lost*, 9 U. CHI. L. SCH. ROUNDTABLE 155, 157 (2002) (summarizing Locke's labor theory of property as "[t]he proposition that property arises from laboring upon things in the world—mixing one's pre-owned labor with unowned things . . . .").

119 *Thyroff*, 864 N.E.2d at 1278 ("We cannot conceive of any reason in law or logic why this process of virtual creation should be treated any differently from production by pen . . . . A document stored on a computer hard drive has the same value as a paper document kept in a file cabinet.").

120 Thyroff v. Nationwide Mut. Ins. Co., 460 F.3d 400 (2d Cir. 2006). The procedural history of this case is complicated. Thyroff initially filed the suit in the U.S. District Court for the Western District of New York, but after dismissal of the conversion claim upon a motion to dismiss, he appealed to the Second Circuit. The Second Circuit then held that whether electronic data can support a claim for conversion is an unsettled question under New York law, but if it could, the district court erred in holding that Thyroff failed to state a claim sufficient to survive Nationwide's motion to dismiss. The court then certified this question to the New York Court of Appeals. *Id.* at 407. The New York Court of Appeals answered the question in the affirmative, *see Thyroff*, 864

against Nationwide, the court ruled that he did not "produce sufficient evidence of demand to survive summary judgment."[121] But how could this be? Louis told Nationwide that he had "lots of personal info on the computer" and that he "want[ed] it back."[122] According to the Second Circuit, his demand was not sufficiently precise; "lots of personal info," according to the court, "could refer to anything from emails to customer lists."[123]

Louis's lack of precision perfectly highlights a much larger problem for data rights. Defining the bounds of a specific intangible digital asset can be incredibly difficult.[124] Defining the scope of digital property rights more broadly is even harder. This is so for two primary reasons.

First, "[t]he amorphous nature of the digital world makes it difficult to define a digital asset."[125] Determining what exactly is owned requires an intimate knowledge of the technologies involved and an informed analysis of the boundary between the digital asset and the operating system or other software on which the asset exists. Imagine a Microsoft Word document. Is the digital asset the bits as they are written on the hard drive? What about the copy that is loaded onto RAM? What about the copy that is uploaded onto Google Drive? Are they all the same asset? Are there now three distinct assets in question? This is not a new or unique perspective. Benjamin Hayward, for example, has noted that "digital products do not form a closed list—the concept itself is hard to define."[126] Warren Agin, too, has noted that electronic "things" such as data "are as hard to define as they sometimes are to understand."[127] Because of these difficulties, some commentators have adopted a functional approach. Rachael Ferrante and Kristina Sherry, for example, have argued that "[f]or lack of a better description, a 'default working definition of digital assets will be anything owned that is in a digital

N.E.2d at 1272, and the Second Circuit then vacated the district court's dismissal of Thyroff's conversion claim and remanded the case to the district court. *See* Thyroff v. Nationwide Mut. Ins. Co., 493 F.3d 109 (2d Cir. 2007). There, Nationwide moved for summary judgment. *See* Thyroff v. Nationwide Mut. Ins. Co., 360 F. App'x 179 (2d Cir. 2010) (affirming district court's grant of summary judgment).

121 *Id.* at 181 ("The purpose of the demand requirement 'is simply "that one in lawful possession shall not have such possession changed into an unlawful one until he be informed of the defect of his title and have an opportunity to deliver the property to the true owner."'" (quoting Leveraged Leasing Admin. Corp. v. PacifiCorp Cap., Inc., 87 F.3d 44, 49 (2d Cir. 1996))).

122 *Id.*

123 *Id.*

124 *See generally* Marinotti, *supra* note 60 (noting that many intangible assets fail the theoretical requisites for property rights, but not because of their intangibility; certain intangible crypto assets, for example, may fulfill these same requirements).

125 Richard Martin & Shannon Noya Nairn, *Estate Planning Guidance for the Protection of Digital Assets*, L.A. LAW., Oct. 2016, at 15.

126 Benjamin Hayward, *What's in a Name? Software, Digital Products, and the Sale of Goods*, 38 SYDNEY L. REV. 441, 454 (2016).

127 Warren E. Agin, *The Internet Bankruptcy: What Happens When the Bell Tolls for the eCommerce Industry?*, 1 J. HIGH TECH. L. 1 (2002).

file.'"[128] This definition, however, would lead us to circular reasoning, defining property in terms of what is owned and defining what is owned in terms of property.

Second, defining digital property is difficult because of the nature of these property rights themselves. Imagine the same Microsoft Word document as above. Does the property right to exclude apply to each copy (i.e., hard drive, RAM, Google Drive) independently? Does it apply to the three as a collective? What happens when one copy is altered slightly? What if only its metadata changes? Is this a trespass to chattel? Defining the rights that align with data as property is just as hard as defining the boundaries of the data itself. The nuances relevant to each asset, each type of data, may not be applicable to all others. Relying on the common law's foundational instruments of stare decisis and reasoning by analogy to define the broad category of data property rights will not yield sufficiently definite or useful rights for the purposes of trust law.[129]

Ultimately, defining data and data rights—whether they are based on personal information, theories of labor, or any other source—will be difficult. Furthermore, such definitions may need to be context-specific depending on the data or digital assets in question. Both of these points make it difficult, if not impossible, for the law of trusts to recognize data trusts without legislative intervention.[130] Although determining the exact legal nature of data is not a prerequisite for the creation of data trusts, these difficulties nonetheless provide unanswered questions that will hinder the adoption of data trusts as a means of private data governance.

III
BACK TO SQUARE ONE?

Despite the difficulties presented in this Essay, the goal of this discussion was not to dissuade further research on the topic of data trusts. Rather, the analysis presented here merely demonstrates that data trusts—as they are currently envisioned—will not be able to bypass legislative intervention through immediate private implementation. If that is the case, however, one must seriously consider whether data trusts are indeed a better

---

128 Rachael E. Ferrante, *The Relationship Between Digital Assets and Their Transference at Death: "It's Complicated"*, 15 LOY. J. PUB. INT. L. 37, 41–42 (2013) (citing Kristina Sherry, *What Happens to Our Facebook Accounts When We Die? Probate Versus Policy and the Fate of Social-Media Assets Postmortem*, 40 PEPP. L. REV. 185, 194 (2012)) (noting that "definitions of what constitutes digital assets vary significantly").

129 At the same time, creating unique solutions for each possible type of digital asset is not only an inefficient use of judicial resources; it may also risk infringing legislative authority.

130 Bypassing the need for legislative intervention is one of the alleged benefits of the data trust approach. Austin & Lie, *supra* note 29, at 618 ("Instead of waiting for the slow process of law reform to create such a regulatory framework, the trust model offers a way of managing these emerging issues through a private law mechanism.").

governance strategy than any other legislatively implementable approach. As Jonathan van Geuns and Ana Brandusescu note in their research for Mozilla Insights, there are many emerging alternative forms of data governance and data stewardship.[131] Among others, data cooperatives, data commons, data collaboratives, data fiduciaries, and data marketplaces all offer methods of regulating the creation, dispersion, and exploitation of data. While each of these methods has "imperfections," all of them aim to "address imbalances of power between data holders and data subjects."[132]

Furthermore, data trusts should not only be compared to such wide-ranging, alternative frameworks; the costs and benefits of data trusts must also be compared to the costs and benefits of the status quo: the evolving distributed system of various data protection regulations such as the CCPA, HIPAA, and the Family Educational Rights and Privacy Act (FERPA).[133]

CONCLUSION

Data trusts have been proposed as a data governance solution that bypasses "the slow process" of legislative law reform.[134] Unfortunately, the analysis put forth in this Essay demonstrates that a legislative solution will nonetheless be necessary to determine the existence and scope of data property rights, even if merely under the requirements of equitable trust law. Before rushing to promote the normative policy benefits of this governance structure, it is crucially important to determine the viability and requisites of its underlying legal infrastructure. Some have proposed software implementation of trust-like governance solutions,[135] or governmental or public-private data-sharing frameworks,[136] or even contracts, as discussed above. But if data trusts are meant to benefit from the body and flexibility of trust law, including its fiduciary relationships, data trusts must be actual trusts. A renewed focus on the underlying infrastructure of trust as a legal instrument is needed before discussions of data trusts can fully explore the normative benefits of this governance strategy.

---

131 *See* MOZILLA INSIGHTS ET AL., *supra* note 33, at 4.

132 *Id.*

133 *See supra* note 110; *see also* 34 C.F.R. § 99.2 (2022) (codifying requirements for the protection of privacy of parents and students).

134 Austin & Lie, *supra* note 29, at 618.

135 Governance of access, use, and profit of data can be technologically assigned through cryptography and smart contracts. *See, e.g.*, *Sightline Innovation Security Products*, SIGHTLINE INNOVATION, https://www.sightlineinnovation.com/product [https://perma.cc/Q42X-BMWR] (describing Sightline Innovation's "audit trail of data usage and enforce[ment of] data usage rights via smart contract").

136 *See, e.g.*, *Silicon Valley Regional Data Trust (SVRDT)*, CTR. FOR COLLABORATIVE RSCH. FOR AN EQUITABLE CAL., https://ccrec.ucsc.edu/partnerships/silicon-valley-regional-data-trust [https://perma.cc/2E85-SHG2] (describing how the "Silicon Valley Regional Data Trust (SVRDT) is a secure cross-sector data-sharing environment combining administrative records from education, health and human services, and juvenile probation in the tri-county Silicon Valley").

Given the rapid expansion of the global datasphere with each passing year, the fervor to address problems of data negligence and malfeasance—as well as the inherent power imbalance between tech companies and the individuals who use them—is both understandable and laudable. Each day over "500 million tweets, 294 billion emails, 4 million gigabytes of Facebook data, 65 billion WhatsApp messages and 720,000 hours of [YouTube] content" are added to the world.[137] By the year 2025, we are expected to create, capture, copy, and consume "a mind-boggling 175 ZB [zettabytes]" of data; to put that in context, one zettabyte is equivalent to 1,000,000,000,000,000,000,000 (10^{21}) bytes.[138] This rapid expansion of the datasphere will only further cement the need for data governance strategies that successfully balance scientific innovation, economic prosperity, personal privacy, and individual autonomy, among the many other interests at stake currently being discussed in this rapidly evolving field of research.[139] Given that data trusts are unlikely to offer refuge from the current legislative gridlock, it is imperative that we develop and pursue doctrinally, legislatively, and technologically implementable data governance solutions.

---

137 Melvin M. Vopson, *The World's Data Explained: How Much We're Producing and Where It's All Stored*, CONVERSATION (May 4, 2021, 11:17 AM), https://theconversation.com/the-worlds-data-explained-how-much-were-producing-and-where-its-all-stored-159964 [https://perma.cc/8Z6K-KUPY].

138 Or the equivalent of 8,000,000,000,000,000,000,000 individual bits of information. *Id.*

139 As the amount of data in the world swells to these astronomical numbers, its economic value—and harmful potential—will only grow. While it is correct to assume that this imminent flood will contain data that is simply industrial in nature (which may also be harnessed for misuse), let us not forget the burgeoning market of Internet of Things devices such as cloud-synced baby monitors, video doorbells, and smart home gadgets as well as the adoption of wearables such as the Apple Watch, Snap Spectacles, the Google Assistant-connected Pixel Buds, and the many fitness trackers entering the market. These represent a growing source of personal data "encouraging mass exploitation of consumer data and posing security threats on an unprecedented scale." Sarah Shyy, *The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business*, 20 U.C. DAVIS BUS. L.J. 137, 139–40 (2020) (discussing specifically how the terms of service agreements provided by Google and Facebook, which users must consent to in order to access their services, have defanged the GDPR).