Essay

In trust, data

Keith Porcaro†

INTRODUCTION

Impermanence is the hidden motif of the digital age. Data and software projects that rise to prominence seemingly overnight can fade just as quickly. Estimations of a dataset's potential value or risk grow stale as technology advances or fortunes change. Promises about the long-term future of digital assets are easy to make and difficult to keep.

Advancing technological capability creates uncertainty for organizations who were not born digital, but who nonetheless must manage and use data and code to advance their missions. Software they depend on can fall out of maintenance. Uncertainty about the long-term value or risk a dataset might yield increases the cost of joining and managing data-sharing collaborations. Data derivatives can be difficult to manage and track.

These less flashy governance challenges struggle for oxygen behind the fiery debate about how to regulate and manage large technology companies and their platforms. But they persist, for civil society organizations, for archivists, for hospitals, and others.

This Essay explores how the trust, and specifically the asset management functions that trust law affords, can be used to ameliorate select digital governance challenges. A trust's ability to isolate assets can protect public interest technology projects against organizational failure, facilitate archiving and study of proprietary and deprecated software, and help multi-party data-sharing collaborations manage complex value allocations. The equitable remedies that a trust makes

† Rueben Everett Senior Lecturing Fellow; Director, Digital Governance Design Studio, Duke Law School. Thanks to Sheryl Groeneweg, Rodrigo Arancibia, and Benoit Leduc at ISED Canada for supporting research that led to an early version of this Essay. Thanks also to Jeff Ward, Anne Tucker, and Sean McDonald for their comments on drafts. All mistakes are my own.

available can facilitate a strong, norm-setting form of data license that enables beneficiaries to claw back unauthorized data derivatives.

Despite discussing cases where data may be trust property, I avoid using the term "data trust" to categorize these applications. First coined by legal scholar Lillian Edwards in a 2004 paper,[1] the term "data trust" has since metastasized to become a catch-all brand for new data relationships, which may or may not implicate trust law or even trust-like relationships. Data trusts are used to describe data-sharing contract standards,[2] to keep owners of a data analysis platform at arm's length,[3] to encourage data sharing,[4] to create friction in data sharing,[5] to describe any fiduciary relationship that relates to data,[6] to facilitate intra-institutional data sharing,[7] to represent pooled interests in personal data,[8] to provide alternate data processors,[9] and so on.

1. Lillian Edwards, *The Problem with Privacy*, 18 INT'L R. OF L. COMPUTERS & TECH. 3, 263 (November 2004). Edwards uses the term "data trust" to describe a common law trust structure that facilitates the redistribution of profits from data collectors and data processors to data subjects. *See generally id.*

2. DAME WENDY HALL & JÉRÔME PESENTI, GROWING THE ARTIFICIAL INTELLIGENCE INDUSTRY IN THE UK 4 (2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf [https://perma.cc/CR35-2GVQ].

3. Paul Meller, *Truata Delivers Next-Generation Data Protection and Analytics to Europe*, BUSINESSWIRE (Mar. 15, 2018), https://www.businesswire.com/news/home/20180315005200/en/Truata-Delivers-Next-Generation-Data-Protection-and-Analytics-to-Europe [https://perma.cc/R3QR-8U9M].

4. Alyssa Harvey Dawson, *An update on data governance for Sidewalk Toronto*, SIDEWALK LABS (Oct. 15, 2018), https://www.sidewalklabs.com/blog/an-update-on-data-governance-for-sidewalk-toronto [https://perma.cc/ST2Y-36Y3].

5. Jack Hardinges, *Data Trusts in 2020*, THE OPEN DATA INSTITUTE (Mar. 17, 2020), https://theodi.org/article/data-trusts-in-2020 [https://perma.cc/5HLT-W5A9]. ("This does not mean that the data trusts we're seeking to bring about will simply facilitate data sharing between organisations, or be more permissive than alternative forms of data stewardship. On the contrary, they will often apply a fairly significant degree of friction to data sharing – establishing where that friction is warranted is a big part of the challenge to be addressed.").

6. *Id.*

7. Marty Graham, *Lessons from a user-trusted data trust*, DELL PERSPECTIVES (Oct. 2, 2019), https://www.delltechnologies.com/en-us/perspectives/lessons-from-a-user-trusted-data-trust [https://perma.cc/5JEA-NA74]; Dr. Christopher Chute, *Data trust*, JOHNS HOPKINS INSTITUTE FOR CLINICAL AND TRANSLATIONAL RESEARCH, https://ictr.johnshopkins.edu/programs_resources/programs-resources/i2c/data-trust [https://perma.cc/PU3Y-JLYH].

8. Sylvie Delacroix & Neil D. Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIVACY L. 236, 237 (2019).

9. *Microsoft Azure Germany Now Available via Innovative First-Of-A-Kind Cloud Model for Europe*, MICROSOFT (Sept. 21, 2016), https://news.microsoft.com/europe/

The "data trust" branding and logic have a simple appeal: to solve irresponsible uses of data, entrust data to someone who is legally required to be responsible for it. To build trust, use a trust.

While acknowledging that a body of law may eventually coalesce around a "data trust" brand, I offer two critiques. First, without a coherent underlying body of law, the broad use of the term "data trust" threatens confusion, wasting the signaling value that trusts can provide. Second, the use of trusts as vehicles for community data protection depends on a rickety structural assumption: that the effects of decisions about data can be confined to a community of data subjects.

This Essay advocates restraint. It argues that the most fitting application of trust law to data and code is via the trust's asset management functions, rather than as a vector for remaking platform-user relationships. Part I of this Essay offers a short introduction to trust law, and considers the practicality of digital trust property. Part II applies a trust's asset isolation capabilities and equitable remedies to particular challenges of digital initiatives and collaborations. Part III warns against the increasingly prevalent "data trust" term, and its inability to meaningfully protect communities from data-driven exploitation. I conclude with a brief reflection on the legal infrastructure new data management paradigms may demand.

I. TRUSTS; DATA AS TRUST PROPERTY

A trust is a legal device for dealing with property for the benefit of another.[10] A trust involves three roles: a settlor, who puts property into trust; a beneficiary, who takes equitable title over the property; and a trustee, who takes legal title over the property.[11] A grant to a trust can be revocable or irrevocable.[12] Each role in a trust need not be played by a separate party, except that a beneficiary cannot be the sole trustee.[13] A trust creates a fiduciary relationship, where the trustee is duty-bound to manage the trust property to benefit the beneficiary or beneficiaries, who may otherwise be vulnerable to misappropriation of trust property.[14] A trustee's duties are defined in trust law,

2016/09/21/microsoft-azure-germany-now-available-via-innovative-first-of-a-kind-cloud-model-for-europe [https://perma.cc/2FFP-DUE5].

10. RESTATEMENT (THIRD) OF TRUSTS, § 2 (AM. L. INST. 2003) (hereinafter RESTATEMENT THIRD).

11. *Id.* § 3.

12. *See generally id.* § 11

13. *Id.* § 3 cmt. b

14. *Id.* § 2 cmt. b; *see also* John H. Langbein, *The Secret Life of the Trust: The Trust as an Instrument of Commerce*, 107 YALE L.J. 165, 182 (1997).

which establishes defaults of loyalty and prudence (among others), and in the trust document, which can override some defaults and establish additional duties.[15] The trust document plays a dominant role in defining a modern trust and the duties of a trustee.[16] The term "trust" is sometimes used to refer to other "relationships or arrangements" which may not actually be trusts.[17] Although they may borrow from trust law, they are governed by separate bodies of law.[18] This essay uses the term trust to refer to the legal instrument.

A trust allows a settlor to delegate the ongoing management of an asset. A settlor can use a trust to isolate a subset of assets to be professionally managed in transactions with third parties.[19] A trust structure isolates the settlor from liability related to the asset's management, while also ensuring the asset is protected from the manager's insolvency.[20] Trust law also enables a settlor to recover improper purchases or transfers of the assets along with any related income.[21]

The basic framework—using a trust to direct and constrain the power of a semi-autonomous expert manager—has become a popular approach for complex asset management.[22] Settlors can use a trust to set and direct long-term goals for an asset and its derivatives. Multiparty collaborations around shared property can use a trust to reduce negotiating and maintenance costs that may arise in contracting and enable complex value allocation structures.[23]

Any property can be trust property, digital or not.[24] While typically applied to monetary, tangible, and intellectual property interests, a trust's asset management functions can also prove useful for managing select digital property interests. Whether data, especially personal data, should be considered property is the subject of

15. RESTATEMENT THIRD § 4 cmt. a(1).

16. *See id.*

17. RESTATEMENT THIRD § 5 cmt. l.

18. *Id*.

19. *See* Henry Hansmann & Ugo Mattei, *The Functions of Trust Law: A Comparative Legal and Economic Analysis*, 73 N.Y.U. L. REV. 434, 470 (1998).

20. *Id.* at 468.

21. *Id.* at 463.

22. *See* Langbein, *supra* note 14, at 168–71; Steven L. Schwarcz, *Commercial Trusts as Business Organizations: Unraveling the Mystery,* 58 BUS. L. 559, 559–60 (2003); Robert Sitkoff, *An Agency Costs Theory of Trusts Law*, 89 CORNELL L. REV. 621, 633–34 n.55, 57 (2004).

23. *See* Anthony Ogus, *The Trust as Governance Structure*, 36 U. TORONTO L.J. 186, 187–88 (1986).

24. *Id*. §§ 40–41.

continued debate.[25] We need not resolve the issue here. For our purposes, it is sufficient to ask whether it is possible to represent a given dataset in terms of ascertainable property interests (we can obviously do so for code and other digital assets). Under current law, with some exceptions, the answer is generally yes. A specific instance of data—a database stored on a server or a cloud service—can be ascertainable as property. So too could the rights to access or query a data source or a continuing stream of data be considered trust property.

Data's fungibility and representative nature raise *practical* challenges for management in a trust, not legal ones. While any data could be included in a trust, it may be practically difficult for a trust to manage data if the information the data represents can be obtained via parallel methods, or if the settlor lacks a monopoly over the data source.[26] While trusts may be poorly suited for protecting easily duplicated personal data, they are well-suited for helping direct the long-term management of certain digital assets.

II. ISOLATING DIGITAL ASSETS; RECLAIMING DATA DERIVATIVES

Two attributes of trusts can help organizations build resilient management for digital assets: isolating assets, and equitable remedies. A trust's asset isolation functions can help preserve a digital asset's long-term use or facilitate complex value allocations for data-sharing collaborations. When deployed as a form of license, a trust could help prevent unwanted uses for digital assets, and help beneficiaries claw back data derivatives.

A. TRUSTS CAN ISOLATE DIGITAL ASSETS, HELPING TO SECURE LONG-TERM USES.

Trusts isolate assets from settlors. A trust can protect a settlor from liabilities and risks related to the property in trust.[27] Conversely, a trust can protect trust property—and the settlor's long-term intention for it—from risks and liabilities related to the settlor or the trustee, such as insolvency.[28]

While risks are often described in terms of pecuniary losses or creditor claims, irrevocable trusts can also isolate an asset from the

25. *See, e.g.*, Salome Viljoen, *Data as Property?*, PHENOMENAL WORLD (Oct. 16, 2020), https://phenomenalworld.org/analysis/data-as-property [https://perma.cc/PR8Z-3KBY].

26. *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy,* 117 COLUM. L. REV. 1369, 1443 (2017).

27. *See* Hansmann & Mattei, *supra* note 19, at 461; Schwarcz *supra* note 22, at 566.

28. *See* Langbein, *supra* note 14, at 173, 179–80; RESTATEMENT THIRD at § 31.

changing interests of a settlor. A trust can capture a settlor's (or settlors') intent at the moment of creation and preserve it in the face of changing circumstances. As a dataset's benefits and risks mutate with technology's advance, this can be an especially useful attribute. In addition to its substantive functions, isolating assets via trust can signal that an asset will continue to be managed exclusively for the purposes defined in the trust document, isolated from interfering interests, and protected by a committed fiduciary.

Beyond risk management, a trust's asset-isolating features can also enable more flexible allocations of interests. Trusts can securitize an isolated asset, and permit value allocation structures that may not be possible with corporate forms, which have formal roadblocks that can inhibit the creation of new shares or classes of shareholders.[29] In a master trust, for example, multiple classes of beneficiary interests are issued on a common pool of assets, each with different substantive rights, risk profiles, and allocative entitlements.[30] These classes do not have to be defined in advance: a settlor can define a default set of beneficiary rights in a trust document, and allow a trustee to continue to create new classes of beneficiaries after the trust is organized.[31] A trustee's default duty of impartiality positions them to navigate and resolve conflicts of interest among beneficiary classes.[32] Applied to digital assets, a trust's asset-isolating features could be used to help ensure the continued availability of data and code, to facilitate the study of proprietary digital artefacts, and to enable complex value allocations for multi-party data collaborations.

1. Ensuring the continued availability of data and code.

The simplicity of accessing data and software belies the fragility of digital infrastructure: data and code that non-technical communities rely on, but may be unable to replicate. Failed and abandoned technology projects are common. While some failures are due to a lack of user interest, even popular projects may fail due to financial instability. Public interest technology projects are especially susceptible—they rely on fickle philanthropic funding that can be unrelated to the project's uptake and may be hosted at organizations with experimental business models. When public interest technology projects

29. *See* Schwarcz, *supra* note 22, at 566-68; Langbein, *supra* note 14, at 183–85; *see also* Sheldon A. Jones, Laura M. Moret & James M. Storey, *The Massachusetts Business Trust and Registered Investment Companies*, 13 DEL. J. OF CORP. L. 421, 455 (1998).

30. *See* Schwarcz, *supra* note 22, at 567–68 (describing a master trust).

31. *Id*.

32. *Id*. at 577–79.

fail, the nonprofit organizations and constituent communities who rely on them are left vulnerable.

Open-sourcing alone may not ensure a project's continued maintenance or the continued availability of a software service—the community is itself attempting to repair the disconnect between a given project's popularity and monetary support for its maintenance.[33] The rise of software-as-a-service models has led some nonprofit technology projects to move away from open-source, for fear of enabling for-profit competitors.[34] The risk of failure is not limited to software projects. Research or data without a clear monetary value may meet an unpredictable fate in a wind-down or bankruptcy proceeding, if it is not simply deleted.[35] Even government-sponsored data is not immune: consider the rush to save government-hosted climate data in 2017.[36]

Failures may not be preventable, but their impact can be mitigated. A trust could be used to create a sort of living will for a digital project. A copy of a digital project's assets could be placed in trust, where a trustee would be tasked with finding a new steward for the project's purpose if the settlor closes the project, files for bankruptcy, or triggers some other condition in the trust document. Because data and code are nonrival goods, this structure need not inhibit alternate uses of the data and code.[37] Funders or operators of public interest data and technology projects could adopt this model as a safeguard for high-risk grantees, or to signal to potential users that a project is "safer" to rely on.

2. Archiving and study of proprietary digital artefacts.

Technology's advance threatens our ability to archive and study digital artefacts, which may rely on deprecated but still copyrighted

33. *See* Josephine Wolff, *What Heartbleed Taught the Tech World*, SLATE (Oct. 22, 2019, 8:20 PM), https://slate.com/technology/2019/10/heartbleed-lessons-open-source-code.html [https://perma.cc/5K72-CD4K].

34. *See, e.g.*, Dean Jansen, *Why We are Closing Amara's Source Code*, AMARA (Jan. 13, 2020), https://blog.amara.org/2020/01/13/why-we-are-closing-amaras-source-code [https://perma.cc/LL2J-GFCM].

35. *See* Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy,* 44 WM. & MARY. L. REV. 1801, 1821–40 (2003).

36. Zoë Schlanger, *Rogue Scientists Race to Save Climate Data from Trump*, WIRED (Jan. 19, 2017, 9:00 AM), https://www.wired.com/2017/01/rogue-scientists-race-save-climate-data-trump/ [https://perma.cc/T7SN-SRRZ].

37. This strategy could also be deployed as a "poison pill" for proprietary projects with defined social missions: if the project deviates from its mission, the trust seeds its competitors.

software or hardware—from video games and digital art to computer-aided design software and architectural plans.[38] This problem is not limited to commercial technology: the deployment of proprietary decision-support systems inside government inhibits future efforts at study and accountability.[39] As technology companies come and go, and as software moves away from downloaded copies and into the cloud, an orphan works problem for the digital age is emerging, where the preservation, study, and use of digital artefacts is stymied by an inability to locate rightsholders.[40] In the case of cloud software, the potential problem is starker: it may be nigh-impossible to recreate a digital artefact or its supporting services.

Trusts are often used to isolate a subset of a settlor's assets and manage them in transactions with third parties. Here, a rightsholder could use a trust to put digital assets in a sort of escrow, to allow for future study and audit of proprietary data and code. Libraries could use this structure to accumulate archiving and study rights for proprietary digital artefacts, protecting future scholars from having to track down and negotiate with rightsholders, or gamble on a fair use defense.[41] A trust structure could help signal that the escrowed assets will not be used to compete with the settlor's business interests.

3. Complex value allocations for multi-party data collaborations

It is difficult to project where new inferences and discoveries may arise from an individual dataset. In data-driven collaborations, where multiple stakeholders contribute data and resources to advance open-ended research goals, data's uncertain potential can bedevil efforts to fairly allocate value that the collaboration produces. In effect, a data-driven collaboration is a joint venture with not only an uncertain return and multiple potential classes of beneficiaries, but an initial investment of uncertain value.

38. *See* U.S. Copyright Office, SECTION 1201 RULEMAKING, SEVENTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION 230–82 (2018).

39. *See, e.g.*, Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L. J. 797, 799–805 (2021).

40. *See generally* David R. Hansen, Kathryn Hashimoto, Gwen Hinze, Pamela Samuelson, and Jennifer Urban, *Solving The Orphan Works Problem for the United States*, 37 COLUM. J.L. & ARTS 1, 4–14 (2013).

41. This and the previous example are similar to source code escrows used in commercial software licensing to protect against a vendor closing (or other contractual violation). A trust can facilitate escrow-like situations where there is not an obvious receiving counterparty.

Take health data collaborations. Health systems may build inter-institutional data-sharing collaborations to advance research and quality improvement goals.[42] The members of these collaborations may also compete with one another—for research dollars, for patients—even on the very subject of the collaboration. This competitive tension combined with data's uncertain potential can create value allocation challenges. Health data collaborations may struggle to allocate ownership of new inferences and discoveries, much less forecast that ownership in advance. Collaborative data networks with dozens or hundreds of participants may require flexible value allocation models that are customized on a per-discovery basis. This may be too complex for a traditional shareholder arrangement and may be too difficult to manage with contracts alone.

While alone not sufficient to overcome actual distrust issues between parties, a trust's flexible value allocation structure and a trustee's duty of impartiality could help reduce friction in complex data collaborations. A trustee could distribute value to collaborators based on their determined contributions to a discovery, as the discoveries happen. New collaborators could be added to the trust over time, as part of new or existing beneficiary classes, each with different rights and allocative entitlements.[43] Because data is an essential ingredient of uncertain value, a trustee could serve as an independent, impartial assessor of a dataset's post hoc value, and each collaborator's stake in the resulting venture.

A trust is not strictly necessary to accomplish any of the underlying goals described here: organizations can wind down gracefully, companies can make deprecated software available for study, data collaborations can find common ground. But a trust structure can potentially reduce friction and uncertainty inherent to each of these scenarios.

B. TRUSTS FEATURE STRONG EQUITABLE REMEDIES THAT CAN BE LEVERAGED TO CONTROL DATA DERIVATIVES.

Trusts can facilitate equitable remedies that enable beneficiaries to recover models and derivatives improperly developed from licensed data.

42. *See, e.g.*, Mario T. Britto, Sandra C. Fuller, Heather C. Kaplan, Uma Kotagal, Carole Lannon, Peter A. Margolis, Stephen E. Muething, Pamela J. Schoettker & Michael Seid, *Using a Network Organizational Architecture to Support the Development of Learning Healthcare Systems*, 27 BMJ QUALITY & SAFETY 937, 939 (2018).

43. *See* Schwarcz, *supra* note 22, at 567; Ogus, *supra* note 23, at 205.

Trusts have strong protections against trustees using trust property for personal gain, or for any interest outside of the beneficiary's.[44] The remedies available are equitable:[45] a beneficiary can enforce a constructive trust against subsequently acquired property;[46] follow trust property into its product;[47] trace commingled trust property in the case of fungible items;[48] recover derivatives created or income derived from trust property;[49] or seek specific reparation if reasonable.[50] These remedies apply even if the beneficiary did not suffer harm. If a trustee improperly uses $10,000 of trust monies to purchase a plot of land, and then sells the plot of land for $15,000, the profits belongs to the beneficiary.[51]

How could this be applied to data or digital assets? A trust could facilitate a more stringent version of a data license, especially for data with weak underlying copyright protection. A would-be licensee of a dataset would instead be a trustee. A would-be licensor would be both settlor and beneficiary.

The settlor/beneficiary could use this model to claw back unauthorized derivative products created from the licensed dataset: statistical analysis, machine learning models, software. A beneficiary could also unwind commingled data or force the retraining of models without commingled data. While the deletion of machine learning models is being explored as a regulatory remedy for data misuse,[52] a trust could make the remedy more broadly available, without requiring the offended party to prove harm.

Already, there are hints of this approach. The Structural Genomics Consortium (SGC) used a trust to license reagents: substances used to facilitate other chemical reactions.[53] Licensees of reagents

44. RESTATEMENT THIRD, § 78.

45. RESTATEMENT (SECOND) TRUSTS, § 197 (AM. L. INST. 1957) (hereinafter RESTATEMENT SECOND).

46. *Id.* § 202.

47. *Id.*

48. *Id.* § 202 cmts. h, o.

49. *Id.* § 202.

50. *Id.* § 208 cmt. e.

51. *Id.* § 205.

52. *See Everalbum, Inc.; Analysis of Proposed Consent Order To Aid Public Comment*, F.T.C., 86 Fed. Reg. 6888–91 (January 25, 2021).

53. Aled Edwards, Max Morgan, Arij Al Chawaf, Kerry Andrusiak, Rachel Charney, Zarya Cynader, Ahmed ElDessouki, Yunjeong Lee, Andrew Moeser, Simon Stern & William J. Zuercher, *A Trust Approach for Sharing Research Reagents*, 9 SCI. TRANSLATIONAL MED. 392 (2017); *see SGC Open Science Trust Agreement*, STRUCTURAL GENETICS CONSORTIUM, https://www.thesgc.org/click-trust [https://perma.cc/42PT-EBTZ]; *see also*

were considered to be trustees and obligated not to seek intellectual property protection for any *use* of the reagents—the underlying work that licensee/trustees used the reagents to facilitate were unencumbered by any restrictions.[54] A trust structure enables SGC, as settlor and beneficiary, to claim and open any IP rights that a licensee/trustee tried to create.[55] But by their own admission, the value of the trust is not solely in its power as an enforcement tool, but as a norm-setting influence.[56]

So too for data. A trust is not a structurally invulnerable way to limit unwanted uses of a dataset—would-be users may be able to obtain parallel access to the information the data represents, or a third-party could make a bona fide acquisition from the trustee without being aware of the trust.[57] But it may have signaling value independent of its enforcement value and could encourage better norms for the community built around the dataset in trust. A trust structure could help communities with sensitive data, such as legal aid, build protective research relationships.

III. DATA TRUSTS; A WARNING

"Data trust" is an increasingly prevalent term with inchoate meaning, beyond perhaps fiduciary management of pooled personal data rights.[58] It may be that the term is suffering from definitional growing pains typical of a nascent movement in law. Nonetheless, I offer two brief critiques: a framing critique as applied to the wide use of the term, and a structural critique as applied to models that hope to use trusts for protecting personal data from misuse.

First, the term data trust may confuse users, wasting the signaling value of a trust. While the term "trust" is not exclusive to trust law, other uses of the term tend to be supported by an underlying body of law, and a coherent legal model.[59] No such body of law yet exists for data trusts, and trusts alone offer considerable flexibility in form and function, not all of which may benefit a would-be data subject or trust beneficiary. The lack of clarity around the term "data trust" could lead users to expect a fiduciary relationship of a data trust where none is

David E. Winickoff & Richard Winickoff, *The Charitable Trust as a Model for Genomic Biobanks*, 349 NEW ENGLAND J. OF MED. 1180 (2003).

54. *Id*.
55. *Id*.
56. *Id*.
57. RESTATEMENT SECOND, § 284.
58. *See supra* notes 2–9.
59. RESTATEMENT THIRD, § 5 cmt. l.

present, a set of rights that may not be available, or protections that may not be possible.

Second, a "data trust" structure loses its effectiveness when data and decisions about data can escape the trust confines. Put another way, a data trust for pooled personal or community data cannot guarantee that the effects of its decisions will be confined to its beneficiary data subjects, or that its beneficiaries will be protected from the decisions of other data subjects (or other data trusts).

Take a community of patients who share a chronic condition, who contribute data to a common registry and make decisions about how to use it.[60] Predictive models developed from the community's data could be used to influence protocols for triage and care. Some models could also expose patients to risks, not only related to biased care, but social and economic discrimination based on inferences about their health status.[61]

But were those models to be developed, their influence and risks are borne not just by patients who participate in the registry—but by *anyone* who can be correlated with registry patients, such as people who share the same condition. The activities of the registry can affect patients beyond it, even if they participated in a registry that was more guarded with their data, if they refused to be included in any registry's activities, or even if they were unaware the registry existed in the first place.

Data's power—and risk—comes from the ability to use a sample to make inferences about a class or population.[62] This characteristic threatens privacy, consent, and data protection paradigms, and

60. *See* Britto et al, *supra* note 42.

61. For example, a model to predict a person's risk of Alzheimer's disease or other neurological illnesses based on writing could be used in preventive care, or in automated job screeners. *See* Gina Kolata, *Alzheimer's Prediction May Be Found in Writing Tests,* N.Y. TIMES (Feb 1, 2021), https://www.nytimes.com/2021/02/01/health/alzheimers-prediction-speech.html [https://perma.cc/S5X6-PKST] (describing a predictive model). *See also* Sharona Hoffman, *Big Data's New Discrimination Threats: Amending the Americans With Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease, in* BIG DATA, HEALTH LAW, AND BIOETHICS 85 (I. Glenn Cohen et al. eds., 2018) (describing social and economic discrimination risks from health data).

62. *See* Salome Viljoen, Democratic Data: A Relational Theory for Data Governance (Nov. 11, 2020). Yale L.J. forthcoming (unpublished manuscript) (manuscript at 3–9) (available at https://ssrn.com/abstract=3727562); Nathaniel Raymond, *Reboot Ethical Review for the Age of Big Data*, 568 NATURE 277, 277 (2019); Ignacio N. Cofone and Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1505, n.118 (2018).

challenges efforts to build collective bargaining units for personal data.[63] Trust law does not solve this problem.

CONCLUSION

This essay has demonstrated how trust law might be wielded to solve select digital asset management challenges and support new data management norms. While branding should not run ahead of law, new approaches for stewarding data and digital projects are continuing to emerge, implicating old and new bodies of law.

This movement will demand new legal customs and infrastructure. A trustee's fiduciary duties, built for money and real property, might not map cleanly to digital issues, or to the different contexts that data is upending: a health data fiduciary and a transport data fiduciary might resemble one another in name only. And new data management structures are sure to yield data management disputes.[64] A future of data adjudication may eventually demand a specialized judiciary—a sort of "digital chancery" court to arbitrate disputes and refine evolving duties of care for data management.

Still, even now, trusts can help non-technical organizations ensure that their missions endure, even as they navigate an increasingly uncertain digital world.

63. *See* BIG DATA, HEALTH LAW, AND BIOETHICS 3–6 (I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena & Urs Gasser, eds. 2018); *see also* Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Procedural Privacy Protections,* 57 COMMS. OF THE ACM 31, 32 (2014); Arvind Narayanan & Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information",* 53 COMMS. OF THE ACM 24, 25–26 (2010). *See also* Elvy*, supra* note 26, at 1426–28.

64. *See also* Sean McDonald, *A Novel European Act of Data Governance*, CTR. FOR INT'L GOVERNANCE INNOVATION (Dec. 15, 2020), https://www.cigionline.org/articles/novel-european
-act-data-governance [https://perma.cc/XRT8-6GH9], (describing an "access-to-justice gap in data governance.").