UC Law Business Journal

Volume 20 | Number 2 Article 3

7-2024

From Data Co-opting To Data Co-oping: Using New Corporate Structures, Data Corporate-hood, And Data Personhood To Prioritize Data Privacy

Jonathan Askin

FROM DATA CO-OPTING TO DATA CO-OPING: USING NEW CORPORATE STRUCTURES, DATA CORPORATE-HOOD, AND DATA PERSONHOOD TO PRIORITIZE DATA PRIVACY

*Jonathan Askin**

ABSTRACT

The stakes of information ownership and control have risen dramatically since the Supreme Court's decision in Dobbs v. Jackson Women's Health Organization,[1] after which tens of millions of people in the United States recognized that companies harvest massive swathes of data incidental to our activities and that seemingly innocuous information, such as rideshare or location data, credit card payments, or even monthly cyclical health trackers (i.e., menstruation or birth control) could potentially expose them to civil or criminal liability when linked to a chain of causation in jurisdictions penalizing voluntary abortion.[2] Data scientists recognize the scale, scope, and massive power of corporate and governmental data and meta data access. Legal scholars recognize and debate the Fourth Amendment and other Constitutional implications of data handling by corporate and government actors. Out of view of most legal and data scholars, however, are corporate and other legal frameworks capable of empowering natural persons to exercise greater control over their personal data and metadata through modification of existing, and creation of new, corporate structures and redefining the nature of data.

In response, this Article proposes a US-focused legal framework approach to empower natural persons to take greater control over the corporate and governmental exploitation of their personal data and metadata primarily through the use of existing, but underutilized, legal structures such

* Professor of Clinical Law, Brooklyn Law School; Founder/Director of the Brooklyn Law Incubator & Policy Clinic (BLIP), Innovation Catalyst for the Center for Urban Business Entrepreneurship (CUBE), and Founder, Brooklyn Justice Lab. The author is grateful to Mark Potkewitz, Adjunct Professor of Clinical Law at Brooklyn Law School, and to Beatrice Rubin, Brooklyn Law School Class of 2024, for their support and insights. The author would also like to acknowledge the support provided by Brooklyn Law School's Summer Research Grant Program.

1. *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 (2022).

2. *See Human Rights Crisis: Abortion in the United States After Dobbs*, HUM. RTS. WATCH (Apr. 18, 2023, 12:01 AM EDT), https://www.hrw.org/news/2023/04/18/human-rights-crisis-abortion-united-states-after-dobbs.

as data trusts or data co-ops. The Article explores notions of information ownership, information control, and information distribution since the harnessing of electronic transmission systems through cycles of technological change with a focus on individuals' privacy from corporate and government surveillance. Increasing reliance on technology, both to power and to participate in the contemporary economy and social systems, has required increasingly more interaction with ubiquitous, constantly-connected systems. Such constant interaction and connectivity has provided both private industry and government the opportunity to collect information, both in service of our wants and desires but also to mine, digest, analyze, and exploit how we interact with those systems in service of corporate or government objectives and against the interests of consumers and users. Companies that offer consumers goods and services harvest, not only our communications and correspondence, but also data incidental to our activities, such as information about our physical locations, devices, and networks. The more information about us that is held by others, the more concerning the patchwork of laws, regulations, and common law doctrines that allow for government (as well as corporate and even tech-savvy individuals with selfish, mercenary, or even nefarious, motives) to gain access to information created by and about us, particularly in terms of data held by third parties (i.e., communications network operators and online Internet platforms). However, well-tested legal structures such as trusts or cooperatives, or even modified versions of traditional corporate structures such as C-Corps, LLCs, non-profits, and variations of social enterprises, may empower individuals and community groups to reclaim control over how the data they generate may be collected, stored, analyzed, synthesized, shared, and used. This article proposes that we could establish new-fangled corporate structures, like the Data Co-op, the D-Corp, or the D-LLC, structures that might help to advance data protection in the digital age. Various corporate and quasi-corporate forms, built on concepts of trusts, fiduciaries, and cooperatives, could enable a more collaborative and more accountable approach to data control than traditional corporate forms provide and could better serve to protect individual privacy from corporate and government surveillance and misuse.

Finally, there are profound and evolving concepts surrounding the nature of data, virtualism, and personhood that might inform a new understanding of the nature of data in the digital age and the rights that would inure to data and to virtual and digital persons. To date, legal scholarship has barely scratched the surface of end-user data empowerment through concepts of data corporate-hood and data personhood as means to protect data privacy.

TABLE OF CONTENTS

I. INTRODUCTION

Depending on societal choices, technology may be used to advance centralized control or to advance individual empowerment.[3] Technology may solidify the power of autocrats and corporate powerbrokers, or it may help to increase human agency and spread prosperity. This has certainly been the history of electronic communications networks, from the telegraph to the telephone to the radio to the television to the Internet.[4] Since the emergence of the Internet and the harnessing of digital technology and distribution systems, there has been a battle between the edge (users) and the hub (network and systems operators and platforms) to control the flow of content, data, communications, and the user experience. In each iteration of this battle, the edge seems to gain the early advantage, but almost always, the hub has prevailed.[5] Today, most academics, policymakers, and other authorities tend to agree that Internet platforms and their marketing and corporate clients and partners have inordinate control over access to the flow of user data and that

3. DARON ACEMOGLU & SIMON JOHNSON, POWER AND PROGRESS: OUR THOUSAND-YEAR STRUGGLE OVER TECHNOLOGY AND PROSPERITY (Public Affairs, 1st ed. 2023).

4. NIALL FERGUSON, THE SQUARE AND THE TOWER: NETWORKS AND POWER, FROM THE FREEMASONS TO FACEBOOK (Penguin Press, 1st ed. 2018).

5. Think about the early days of radio broadcast technology in the early part of the 20th century when anyone with an idea and a transmitter could broadcast their content to as many receivers as existed within the reach of the transmitter. *See* John K. Hutchens, *Notes on the Late Dr. John R. Brinkley, Whom Radio Raised to a Certain Fame*, N.Y. TIMES (June 7, 1942). Along came the budding radio empires and the rollup of content, talent, and hardware. We also saw government efforts to regulate use of spectrum as a scare resource and public good. *See* Patrick R. Parsons, *Two tales of a city: John Walson, Sr., Mahanoy City, and the "Founding"; of Cable TV*, 40 J. BROAD. & ELEC. MEDIA 354 (1995). In more recent decades, we've seen the battles between pirate radio, licensed radio, and government agencies battle over the acceptable uses of spectrum. We've seen similar battles over eyeballs in the world of video content distribution, from the early days of television into the early days of cable and the battles over content control and distribution. More recently, we've witnessed the battles between the peer-to-peer renegades like Napster and the media conglomerates trying to maintain control over content creation and distribution. *See* Randy Kluver, *Globalization, Informatization, and Intercultural Communication*, 3 AM. COMMC'N J. 425 (2000).

the online experience often negatively affects both our online and offline experiences — although few viable solutions have been deployed to curb this degree of corporate control.[6] Policymakers and citizen advocates are just starting to recognize what data scientists and the Internet access and service providers have known for decades: by harnessing our data and metadata, these corporate actors can digest, analyze, and synthesize the universe of individual data and metadata and may now direct and modify our proclivities, psyches, and actions in ways never before available in all of human history.[7] So far, we have only seen the camel's nose under the tent when it comes to the ability of corporations and governments to build psychic models of each of us and to exploit us, both individually and collectively, based on this virtually perfect data-created understanding of us. With the litany of privacy-related opinions, from *Carpenter v. United States*,[8] to *Dobbs v. Jackson Women's Health Organization,*[9] Americans have begun to understand how our "always on" lives may feed the corporations and governments with vast, seemingly disconnected data points that might be used to control our thoughts, behavior, and actions.

Data may be used to improve our lives and society. Data, however, may also be used against our will and better interests. Balancing the beneficial effects of data usage with the privacy interests of citizens will continue to be among the most pressing issues confronting us.[10] Much data governance scholarship focuses on reining in the exploitation of user data by corporate and government actors through Constitutional jurisprudence.[11] Some data scientists tout the potential benefits (while also acknowledging the potential harms) of harnessing user data.[12]

Legal scholarship, however, has not explored how evolving concepts of corporate structures might pave the way for both better harnessing of user data, both individualized and aggregated, and for user data protection from unwanted corporate and government surveillance and exploitation. Over the past forty years, we have seen the emergence of new corporate structures, most notably variations of the relatively flexible Limited Liability Company ("LLC") and socially virtuous social enterprises, to modify the processes and goals of

---

6. Dipayan Ghosh & Nick Couldry, *Digital Realignment Rebalancing Platform Economies from Corporation to Consumer* 16 (Harv. Kennedy Sch., Mossavar-Rahmani Ctr. Bus. & Gov't, Working Paper No. 155, 2020), https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_155_final2.pdf.

7. Chris Conley, Metadata: Piecing Together a Privacy Solution (ACLU N. Cal., 2014), https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf.

8. *Carpenter v. United States, 585 U.S. 296, 301–302 (2018).*

9. *Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022).*

10. Janna Anderson & Lee Rainie, *As AI Spreads, Experts Predict the Best and Worst Changes in Digital Life by 2035*, PEW RSCH. CTR. (June 21, 2023), https://www.pewresearch.org/internet/2023/06/21/as-ai-spreads-experts-predict-the-best-and-worst-changes-in-digital-life-by-2035/.

11. *See, e.g.*, Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV.. 1007, 1008 (2022).

12. Thomas Hardjono & Alex Pentland, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management* 2 (2019), https://arxiv.org/pdf/1905.08819.pdf.

corporate organizations.[13] None of these new-fangled corporate structures have directly tackled the objective of protecting user data against unwanted handling by corporations and governments or maximizing the economic and social value of data for the benefit of the end users. This Article is the first to propose multiple vehicles for greater control and use of data through modified corporate structures and emerging understandings of the nature of data, through which users would gain greater control to self-determine the uses of their data, providing users with legally—or at least contractually—required notice, choice, transparency, and consent.

This Article proceeds in VII parts. In Part I, this Article provides background information about the evolution of the technologies and concepts that frame our current understanding of information systems and the varying abilities of corporate, government, and user control of their communications and data in order for the reader to better understand the technological frameworks governing data control and use. In Part II, this Article explores the current state of digital intermediaries that may, to varying degrees, be authorized by users to handle user data in the best interests of the users and the obligations and benefits arising from such intermediary control. In Part III, this Article considers the current state of Fourth Amendment jurisprudence, the Third-Party Doctrine, and what happens when the government gets involved in end-user data access and control. In Part IV, this Article addresses problems with existing trust and fiduciary models to user data control. Part V explores the emergence and viability of data co-ops, algorithms, and the potential for virtuous use of individual and aggregated data for user and community benefit. Part VI addresses hurdles and questions surrounding data co-ops. Finally, Part VII considers an array of new, modified, and potential corporate structures and concepts that could be established to better prioritize and protect user data. In addition to the data co-op itself, this Section proposes new corporate models such as the "D-Corp", the "D-LLC", and the "*Guardian ad Datum*." Finally, this Section tees up "Data Corporate-hood" and "Data Personhood" as emerging concepts to empower data with the status of legal personhood, with Constitutional and other legal rights to protect data from corporate and government unauthorized use.

II. BACKGROUND

A. The Innovation Cycle

Throughout the evolution of electronic distribution systems, we have seen periodic opportunities for more control and tailoring of content creation, distribution, and reception closer to the user and away from central content creators, controllers, and distributors. We humans started our foray into electronic and digital data control fewer than two hundred years ago with

13. Kate Cooney et al., *Benefit Corporation and L3C Adoption: A Survey*, STAN. SOC. INNOVATION REV. (Dec. 5, 2014), https://ssir.org/articles/entry/benefit_corporation_and_l3c_adoption_a_survey.

rudimentary electronic data transmission systems such as the telegraph for the transmission of place-to-place written words, the telephone for the transmission of person-to-person voice, radio for person-to-person transmission of voice and for place-to-person broadcast of audio content, and then television for the one-way transmission of both sound and video broadcast.[14] Early on, these systems were designed to provide direct communications between two end points either through one-way broadcast transmission or through two-way interactive transmission from place-to-place or person-to-person. Economics quickly led to the creation of centralized, intermediating, hub-to-spoke network architectures to replace direct person-to-person and place-to-place connections. These early networks typically started as small groups of individuals banding together for community-based communications,[15] but quickly snowballed into large corporate enterprises as entrepreneurs cobbled together networks into networks-of-networks, and eventually rolled these networks-of-networks into regional, then national, and finally international corporate conglomerated communications systems. Due to the technological limitations of these early communications systems (*e.g.*, radio, television, telephone), each network tended to enable just those with financial resources, powerful transmission equipment, access to wired infrastructure or spectrum licenses, and technological and business knowhow to control the creation, curation, and distribution of information, content, and communications. The public arguably benefited from improvements in individual access to information, content, and communications through improvements in technologies, economics, and architectures. Radios, televisions, and telephones became more affordable, and use of wired and wireless infrastructure became more ubiquitous. The need for shared phones and reliance on human switchboards gave way to electronic, then digital, switches, allowing for increasingly more direct access to more and more individuals across the economic spectrum and geographic regions until we established near-universal access to broadcast and telecom networks. Centralized telephone switchboards gave way to direct-dial as we saw the evolution of telecommunications networks, which allowed for more functionality between any two user endpoints, but also enabled more control by centralized intermediaries. The networks, equipment, and architecture, due in large part to network effects and economies of scope and scale, further ensured consolidation of control over information, content, and communications creation and distribution within the hands of fewer and fewer

14. This Article uses "transmission" and "broadcast" as distinct concepts, with "transmission" referring to any wired or wireless transmission of electronic signals and "broadcast" referring more specifically to the transmission of content from one transmitter to many receivers.

15. Jon Baker, *Hooked on History: Rural Telephone Companies Kept Farmers Connected*, TIMES-REPORTER (Sept. 13, 2021, 5:01 AM), https://www.timesreporter.com/story/news/2021/09/13/history-rural-telephone-companies-kept-farmers-connected/8259609002/; *History of Rural Telecommunications*, NTCA–THE RURAL BROAD. ASS'N, https://www.ntca.org/ruraliscool/history-rural-telecommunications#:~:text=The%20independent%20telephone%20industry%20began,systems%20emerged%20throughout%20rural%20America (last visited Feb. 1, 2024).

monopoly-tending corporate actors. End users (*e.g.,* citizens, residents, humans) may have benefited from the ubiquity, quantity, and quality of communications content and technology, but end users also lost some sense of control, autonomy, and direct power to communicate their own ideas, content, and information.

With the emergence of the Internet, with its ubiquitous and redundant network architecture, we have witnessed a new ability for any individual (or groups of individuals) to bypass the corporate intermediaries of the 20th century and to create more powerful network effects with more powerful functionality and capabilities as any combination of individuals or groups may communicate directly, asynchronously or synchronously, with any other combinations of individuals or groups without any intermediaries to control the communications and interactions. All we needed were robust wired and wireless transmission facilities, affordable end user equipment, user-friendly software and interfaces, and affordable access to the open Internet.

With the emergence of each new technology, however, corporate actors have fought to create online systems that have allowed them to control access to content creation and the distribution.[16] With this increasing technological capability, these corporate actors have also been able to control the user experience and to gather and to exploit more and more user data. In fact, the gathering and exploitation of user data has emerged as the economic engine of the Internet, digital media providers, and digital transmission systems.

Not only do corporate actors have the ability to exploit user data in more and more powerful manners, but so do government actors, particularly once the data has been obtained by corporate intermediaries, largely as a result of evolving U.S. common law and Constitutional interpretation. Once data is given over "freely" to corporate entities, government actors are able, through a U.S. judicial construct known as the "Third Party Doctrine",[17] to access user data, under the guise that the user no longer has an expectation of privacy or control over their data because the user willingly gave the data to a third-party intermediary. The Third-Party Doctrine essentially eviscerates Fourth Amendment protections against unreasonable search and seizure in any digital or online context under the argument that the user willingly gave their data to an online intermediary and, therefore, the user has abandoned their expectation of privacy and control of their data.[18]

But perhaps there are new and growing opportunities to break this stranglehold by corporate intermediaries over control and exploitation of user data. Today, for both technological and legal reasons, the increasing ability to self-organize and to empower users and user groups to control the flow and uses of individual and collective data is increasingly viable (arguably subject to certain jurisdictionally-based approvals over corporate formation and liability).

16. Internet chat rooms on the open Internet gave way to walled gardens on the emerging World Wide Web.

17. *See infra* Part IV.

18. *Id.*

Such technological and structural user control could be the key to breaking the stranglehold of the Internet platforms and data brokers.

i. Rise of the Planet of the Data

Since the dawn of human, pre-written, oral tradition, there has been a battle for control over the hearts and minds of individuals and communities.[19] This battle has centered around two overlapping conflicts: (1) control over content creation and distribution *to* users and (2) control over user information and data *from* users.

If we were to create a histomap[20] of human control of media over the past five thousand or so years, we would notice ebbs and flows in the media landscape between periods of centralized control over content to periods of individual *self*-control over content. Concurrently, we would also see a general trend towards the greater ability of communities and individuals to distribute more content, more broadly across larger swaths of humanity and geography.

We would also see ebbs and flows over the degree of individual, government, and corporate control over personal privacy, identity, and autonomy. Concurrently, we would see never-ending one-upmanship battles between technologies and processes to enable greater capabilities to gather and harness user data (*i.e.*, tending to *decrease* user privacy) and, conversely, to secure, encrypt, and conceal user data (*i.e.*, tending to *increase* user privacy).

Each time a new technology comes along, there is a scramble between (1) those who would promote the power of the individual to create and distribute content freely and broadly (*e.g.*, the early days of amateur radio or even the early days of the pre-Web, pre-walled-gardened, pre-platformed Internet) and (2) those who would try to control and centralize content creation and distribution (*e.g.*, consolidation of radio and television networks; media mergers and consolidation; Internet acquisitions).[21] There has also been a parallel and corollary scramble across the history of each new technology to protect and to eviscerate individual autonomy and privacy, both for political and corporate purposes. The radio has been both a tool by individuals to share independent thoughts without censorship or a tool by government or corporate actors to control, direct, and condition the populace (*e.g.*, wartime propaganda efforts; corporate advertising campaigns). Encryption technology and government limitations on encryption have been used by various sides to either enhance or to limit privacy. We will undoubtedly see efforts by those that would work to enhance privacy and those that would work to curb privacy to use blockchain technology, artificial intelligence, and quantum computing (and whatever technologies might come next) as technological tools for their

19. Perhaps, it's less a battle and more of a dance marathon, in which the recurring dance move is something like one step forward, two steps back, a sideways zig, a dosido, and a leapfrog forward.

20. A histomap is a visualization showing the ebbs and flows of a concept over time. *See* Nick Routley, *Histomap: Visualizing the 4,000 Year History of Global Power*, VISUAL CAPITALIST (Aug. 5, 2021), https://www.visualcapitalist.com/histomap/.

21. *See supra* note 5.

respective purposes. Ironically, no one except a quantum, artificially-intelligent entity/system/person could logically predict with any likelihood of accuracy what the world will look like once artificial intelligence and quantum computing actually take root.

In pre-historic, tribal villages and other early, closely-knit human communities, the individual had little ability to preserve privacy, primarily due to their size and interconnectedness, not to mention the technological limitations (*i.e.*, analog verbal communications and later rudimentary written communications without easy duplicability or encrypt-ability). By some measure, early stages of industrialization and urbanization made it easier for individuals to maintain privacy within the chaos and anonymity of the crowd. With the advent and harnessing of electronic transmission media and digital technologies and human emergence into what we recognize as the information age,[22] it has become increasingly easier for corporations and governments to track individuals, to collect data, and to create invasive profiles of individuals and communities, regardless of the size or geographic scope of the community.

In early tribal oral traditions, the speaker had almost absolute "technical" control over the production, release, and use of their content — the only vehicle for redistribution being another person's analog, imperfect, interpretation and *re*-creation of the same or derivative content. From the early days of the written word, into what Western society identifies as the Middle Ages, content replication and distribution remained largely in the hands of a small guild or class of literate scribes. With the advent of the printing press, content became dramatically easier to replicate and to distribute, at least among the growing literate classes. Through the 17th, 18th, and 19th centuries, pamphleteers harnessed printing and distribution technologies, fighting for attention by self-publishing and distributing their content,[23] only to be reined in by the newspapers and other media distribution outlets that were able to corral and to monopolize, or at least cartelize, content creation and distribution by establishing the media empires of the 20th century.[24]

Electronic transmission via wireline and wireless networks took more control away from the original content creator of the data and allowed for increasingly greater mass replication and distribution. Digital replication and Internet distribution took even more ownership away from the data originator, while simultaneously giving the creator new opportunities for cheaper and broader *self*-distribution. Early peer-to-peer networks made it almost impossible for the originator to restrain digital replication and control the flow of content and data. This sparked the early Internet battles between content creators, Internet platforms, and peer-to-peer distribution software creators

22. Kluver, *supra* note 19.

23. *See* Jason Peacey, *Pamphlets*, *in* THE OXFORD HISTORY OF POPULAR PRINT CULTURE: VOLUME ONE: CHEAP PRINT IN BRITAIN AND IRELAND TO 1660 (Joad Raymond ed., 2015).

24. UNDERSTANDING MEDIA AND CULTURE: AN INTRODUCTION TO MASS COMMUNICATION 153–193 (Univ. Minn. Libr. Publ'g ed., 2016).

(*e.g.*, Napster, BitTorrent, and other promoters of digital search and distribution). At the same time, digital replication and Internet transmission gave inordinately more power to individuals to create their own content distribution systems (albeit without a viable revenue model), while also dramatically encroaching on the individual's ability to control their own content, information, identity, and privacy as communication flowed across the Internet, which enabled digital tracking of user data.

Most recently, however, blockchain and encryption technologies, without government or corporate oversight or control, seem poised to allow end users to regain control over their data, privacy, identity, and autonomy. In fact, we will likely see growing technological, entrepreneurial, and political battles of one-upmanship between those trying to safeguard or exploit user data by harnessing blockchain technology, artificial intelligence, and quantum computing. Artificial intelligence might tend to enable increasingly more top-down access and control over user data, whose unchecked evolution might lead to the ultimate surveillance state (reminiscent of Jeremy Bentham's *Panopticon*). But blockchain technology might foster self-sovereignty and the ability to secure and self-determine the uses of one's data. At the same time, AI will increasingly allow for exponentially greater content creation while simultaneously increasing the prevalence of deepfakes and mistrust in identity, authorship, factual accuracy, and truth. Additionally, blockchain technology would logically enable a greater ability to secure content and to authenticate provenance without having to verify the creator's identity.[25]

ii. From User Content and Data Control to User Exploitation — The Never-Ending Battle for Control of Users and the Online, and Offline, Experience

Over the course of the past two centuries, in the evolution of electronic and digital distribution systems, we have seen the opportunity for more control and tailoring of content closer to the edge (*i.e.*, the end-user) and away from centralized content creators and distributors. Electronic media creation and distribution largely started with broadcast systems that allowed only those with deep pockets, powerful equipment, and sophisticated technical knowhow to create, curate, and distribute content (*e.g.*, the early days of telegraph transmission into the emergence of radio and television broadcasting). The need for centralized telephone operators gave way to direct-dial as we saw the evolution of telecommunications networks that allowed for more and more control and autonomy by, and more functionality between, any two user endpoints. Now, with the emergence of the ubiquitous, distributed Internet, we have the ability for any individual (or combinations of individuals) to create exponentially more powerful network effects with significantly more robust capabilities and viral reach as any combination of individuals or groups may,

25. Jonathan Askin et al., *Trust in a Trustless System: Decentralized, Digital Identity, Customer Protection, and Global Financial Security*, MIT COMPUTATIONAL L. REP. (Jan. 18, 2022), https://law.mit.edu/pub/trustinatrustlesssystem/release/1.

as a technological matter, communicate directly with any other combinations of individuals or groups without any intermediaries to control the communications and interactions on the open, global (and increasingly *exo*-global, i.e., beyond the confines of earth) Internet. Any individual living in the 21st century has more functionality and greater ability to reach and interact with more people over a broader swath of the planet than the most powerful media empires of the 20th century. For instance, content creators in 2024 have the potential for a broader distribution of their musings than the number of people who consumed the most significant media of the 20th century.[26]

Based on the increasing technological power, the decreasing costs to place this technological power in the hands of individuals, and the ubiquity of electronic transmission networks, it seems like the best bet is on the edge (the users) prevailing against the central servers this time around. But, like Charlie Brown's dance with Lucy van Pelt as Charlie approaches Lucy's football,[27] each time a new online digital technology or process comes along (*e.g.*, peer-to-peer file sharing, torrenting, Voice-over-Internet-Protocol, online encrypted digital lockers, blockchain, quantum computing) a new, often noble, typically naïve, group of challengers, unjaded by historical corollaries and institutional memories, thinks they will logically take down the powerbrokers and the old-line, centrally-controlled, top-down, server-spoke, hub-edge ways of doing business. These would-be disruptors and social entrepreneurs often hope to harness the new technology or process to create user-controlled distributed networks and systems that disintermediate the incumbent overlords and their central servers and clouds.[28]

The early generation of Internet startups (e.g., Yahoo!, AOL, Google, etc.) planned (or, at least, claimed) to disrupt the 20th century media empires for the broader public good.[29] In each instance, the early disrupters either died

---

26. On the social media platform, Instagram, professional football (soccer) player Cristiano Ronaldo has roughly 591 million followers, followed by professional football (soccer) player Lionel Messi with 473 million followers, and actress/singer Selena Gomez has 423 million followers. While each of these individuals was a celebrity before joining the social media platform, Khaby Lame, with 79 million followers, came to fame through posting short, wordless comical videos on the social media platform TikTok where he enjoys a following of over 158.3 million followers. To put this in perspective, Sgt. Pepper's Lonely Hearts Club Band by the Beatles soled 32 million copies, 106 million people watched the series finale of M*A*S*H in 1983. *See* Brian Lowry, *'M*A*S*H' Said Goodbye 40 Years ago, With a Finale for the Ages*, CNN (Feb. 28, 2023), https://www.cnn.com/2023/02/28/entertainment/mash-finale/index.html. NASA estimates that roughly 650 million people watch Neil Armstrong first set foot on the moon. *See* Sarah A. Loff, *Apollo 11 Mission Overview*, NASA (Apr. 17, 2015), https://www.nasa.gov/mission_pages/apollo/missions/apollo11.html. In a week, Cristiano Ronaldo can command more attention than Apollo 11.

27. Pig Head, *Lucy & Charlie Brown Kicking the Ball Compilation - The Charlie Brown and Snoopy Show*, YOUTUBE (Oct. 11, 2020), https://www.youtube.com/watch?v=9ivn0C8oebg&ab_channel=PigHead.

28. Jonathan Askin, *From User Exploitation to Data Coops: The Never-Ending Battle for Control of Users and the Online, and Offline, Experience*, DATA CATALYST INST. (Aug. 25, 2022), https://datacatalyst.org/from-user-exploitation-to-data-coops-the-never-ending-battle-for-control-of-users-and-the-online-and-offline-experience/.

29. *Id.*

(e.g., GeoCities), were absorbed into the old empires (e.g., AOL), or became the new media empires with little regard for the end users beyond productizing and monetizing the users themselves (e.g., Google/YouTube, Meta/Facebook). In many cases, the early disrupters themselves failed to adapt, and so, too, fell victim to emergent technologies that obviated the foundations of their early successes.[30]

Many had hoped that peer-to-peer networks and torrents would disintermediate music, video, and voice service providers (*i.e.*, the record labels, the media companies, the cable and telecom companies).[31] Each time, however, society experienced what turned out to be just a temporary disruption and a false hope of end-user empowerment. Each time, either the old powerbrokers regained control, killed or absorbed the insurgents, or new ventures turned into new behemoths to become the new powerbrokers.[32] For example, Google formed with the noble ambition "to organize the world's information and to make it universally accessible and useful."[33] Google's initial promise was "Don't Be Evil."[34] As Google emerged from its larval stage and looked towards its long-term survivability and growth, Google determined that its most viable path to success required monetizing its users' data and auctioning off that data to the highest bidder (*i.e.*, advertisers).[35]

Rather than adopting an advertising-based revenue model, Google could have pursued alternative business models not based on the exploitation of user data (*e.g.*, a monthly subscription model; a micropayments-based revenue model). Had Google built its business around a micropayments approach — that is, charging users a relatively minimal fee for each search — we would undoubtedly have seen greater innovation in micropayments technologies and processes and less innovation in AdTech technology and payment and brokering systems.

For instance, we might have seen the movie industry grow into a system in which a "producer" (independent of the deep pockets of the Hollywood studios) could crowdfund online (through a wide-net, micropayments campaign that could allow each micro-payment funder to become a micro-producer) to support a unique project. Once the project received the required

30. *See* CLAYTON CHRISTIANSEN, THE INNOVATOR' S DILEMMA WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL (Harv. Bus. Rev. Press ed., 1997).

31. *See* Tom Lamont, *Napster: the Day the Music was Set Free*, GUARDIAN (Feb. 23, 2013), https://www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing.

32. Askin, *supra* note 26.

33. *Our Approach to Search: Maximize Access to Information*, GOOGLE SEARCH, https://www.google.com/search/howsearchworks/our-approach/#:~:text=Google's%20mission%20is%20to%20organize,height%20of%20the%20Eiffel%20Tower (last visited Jan. 28, 2024).

34. Kate Conger, *Google Removes 'Don't Be Evil' Clause From Its Code of Conduct*, GIZMODO (May 18, 2018), https://gizmodo.com/google-removes-nearly-all-mentions-of-dont-be-evil-from-1826153393.

35. Shirin Ghaffary & Alex Kantrowitz, *"Don't Be Evil" Isn't A Normal Company Value. But Google Isn't A Normal Company.*, VOX (Feb 16, 2021, 8:01 AM EST), https://www.vox.com/recode/2021/2/16/22280502/google-dont-be-evil-land-of-the-giants-podcast.

funding, the crowdfunded micro-payment obtained proceeds could be used to produce the film. The film could then be distributed online through a micro-payment, micro-distribution process in which each subsequent individual would serve as a micro-distributor atop the pyramid of their own media empire, and could distribute the film to those within their respective micro-orbits. Subsequently, the next viewer could distribute the film to those within that viewer's orbit, and so on for perpetuity. Each time someone viewed the film due to their recommendation engine and distribution network, each player in the chain of distribution would receive a micropayment. This could function as a virtuous funding/production/distribution/revenue pyramid in which everyone who played a role in the funding, creation, and/or distribution of the film could participate in the process and the micro-payment-based revenue stream. Such a system of funding, creation, and distribution could create a virtuous process that would foster expansive creation and distribution without intermediaries trying to stifle creation or distribution. It would be in the interest of every player in the ecosystem (funders, producers, writers,viewers, and distributors) to want the broadest and deepest distribution of all potential content. Without a viable micropayments system, however, the micropayments tools, applications, and ecosystem has stagnated, while the online advertising model has become the predominant, most financially-lucrative (at least from the perspective of the Internet platforms and service providers) model for the Internet.

Once Google chose to pursue an advertising-based revenue model, it essentially wrote the rules for the Internet, transformed what the Internet could and would become, and sealed the fate of the Internet, or at least the first generation of the Web, as one built around attention, marketing, and a fight for advertising dollars. Facebook and most other social networks and online platforms followed suit and turned their users and their users' data into sellable products for brands and advertisers.[36] With the emergence of new distribution systems and payment mechanisms in Web 2.0 and Web3, through torrenting, peer-to-peer networking, and blockchain, efforts have been made to transform the Internet distribution and revenue model, but no ventures have yet succeeded in any meaningful way to break the stranglehold that Google, the other Internet platforms, and their advertising partners have maintained over the Internet.

And with that development – the ability of central platforms to monetize users and their data – round one in the battle for control of the Internet experience and for control over users' individualized and aggregated data went to the Internet platform ventures.

36. *The History of Facebook: From BASIC to Global Giant*, BRANDWATCH (Jan. 25, 2019), https://www.brandwatch.com/blog/history-of-facebook/.

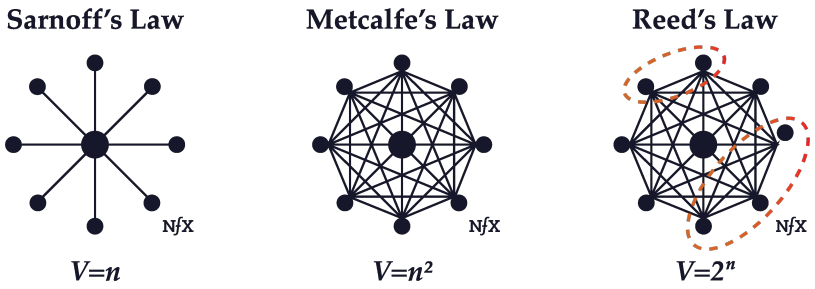
iii. The Power of Networks, Disintermediation, and the Rise of Data Collaboratives

As noted above, there has been a constant back and forth between control of the online experience between end-users and service platforms, with the platforms ultimately winning the battle and creating their own ecosystems through Web 1.0 and Web 2.0. Direct peer-to-peer networking on the open Internet has largely given way to user subjugation to Internet sandboxes and networks controlled by the Internet platforms. Through technological advances with blockchain, artificial intelligence, and quantum computing, the battle will re-emerge as platforms fight for dominance and corral users into their own platforms, metaverses, and other ecosystems. In any case, new technologies, processes, and Internet network models offer potential to establish better structures and systems to control and harness user data for the maximum benefit of users and user communities.

Online networks have the potential to move from the hub and spoke model of Web 1.0 and 2.0, in which the online platforms control the network and user experience, to a disintermediated model, in which control over content distribution and data collection might move to the edge, providing for user *self*-control over content creation and data flow. Admittedly, prior Internet evangelists have attempted to build peer-to-peer networks on the open Internet without involvement of centralized intermediating platforms. Each time, however, the insurgent end-user-controlled networks have been unable to obtain the network effects and viral reach necessary to compete for community against the centralized server platforms (*e.g.*, Facebook and Google).

iv. The Varying Power of Electronic Networks: From Broadcast to Telecommunications to the Internet

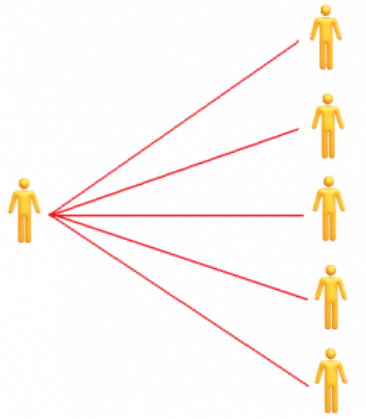
In order to understand the power and potential of the Internet and user control over the Internet experience and data, we should first understand the varying nature and power of the primary electronic transmission architectures. Three "laws" – Sarnoff's Law, Metcalf's Law, and Reed's Law – largely describe the evolution of electronic networks, the value of a network from the perspective of those connected to it, and the ability to put the power of



network effects and reach into the hands of each end user.[37] These three laws describe the power, capabilities, and potential value of a given network based on how participants are connected. What will become obvious through a rudimentary understanding of the varying potential of these networks is the exponentially augmented power of Internet-based networks over traditional broadcast and telecom networks.[38] [39]

Let's consider these network laws from least to most robust:

a. Sarnoff's Law



According to Sarnoff's Law, the value of a network with a single transmitter and multiple receivers is proportional to the number of viewers ((*one* to *many*) with a power equal to *n*, where *n* is the number of users on the network).[40]

Sarnoff's Law describes a traditional radio or television broadcast network. Such a network allows one entity to reach the universe of users within its network (*e.g.*, the reach of a wireless transmitter), but does not allow for users to transmit back to the network or to other end-users on the network. This network essentially only allows for one-way transmission from the transmitter to the receiver and offers no creation or distribution power for the end users themselves.

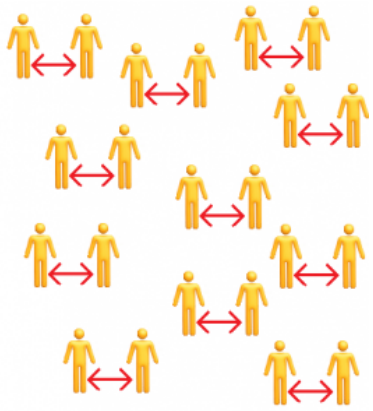
37. Guides Publishing & Muhammad Saad, *The Network "Laws,"* GUIDES PUBL'G, https://guides.co/g/the-network-effects-bible/121725 (last visited Jan. 5, 2024).

38. *Id.*

39. *Id.*

40. Jasper Ong, *The Power and Value of Social Networking*, SOC. MEDIA ONLINE (July 11, 2009), https://socialmediaonline.com/the-power-and-value-of-social-networking/.

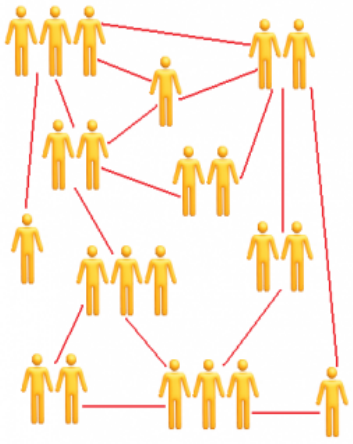
b. Metcalf's Law



According to Metcalf's Law, the value of a network with a hub and spoke model is proportional to the square of the number of connected users of the system ((any*one* to any*one*) with a power equal to n^2, where n is the number of users on the network).[41]

This network is epitomized by the traditional public switched telephone network, which allows any end user to reach any other end user by using the network operator as an intermediary connecting the two endpoints. This network allows for two-way transmission between two end users relying on central switching by a network intermediary. Such a network provides for powerful network effects and control by entities that have the most end users connected to the hub and spoke infrastructure. Large network potential for monopoly control could be mitigated by requirements that network operators interconnect with other network providers.

c. Reed's Law



According to Reed's Law, the power and utility of a network can scale exponentially with the size of the network ((*any* to *any*) with a power equal to 2^n). This network is best epitomized by Internet-based, peer-to-peer networks without (or with limited) intermediary control.[42]

Reed's Law describes the exponential power of Internet-based networks and communications. Each end user or any combination of end users has the immediate power to reach any combination of end users.

On the open Internet, with end-user-friendly architecture and software, without intermediating platforms brokering connections, and with enabling (or, at least, not *dis*-enabling) government regulations, end users and self-organizing groups of end users may self-design and create the rules, parameters, and capabilities of any connections and

41. *Id.*
42. *Id.*

communications, bounded only by the limits of transmission speeds and processing power.

This distinction between Internet architecture and broadcast and telecom network architecture is important because it recognizes that each end-user has exponentially (literally) more power than the most powerful broadcast or telecom network of the pre-Internet Age. The Internet architecture allows for any user or user group to self-create their own rules of engagement and to set the terms of data usage without any platform or hub serving any intermediating function. All the power rests with the end-users to use, reuse, repurpose, and distribute their data as precisely as they dictate with the only limitation being how good the software is to precisely tailor their objectives for the use of data. In turn, all the power rests with the end-users to the extent that government and corporate intermediaries do not limit or corral end-users within limited eco-systems curbing the reach, capabilities, and openness of the Internet.

However, even with the potential for user-created networks on the open Internet, there has been an ongoing effort by Internet platforms to corral user groups within their own Internet sandboxes. There, however, have been periodic efforts by users and social entrepreneurs to push back and disintermediate the Internet intermediating platforms.

As much as we might like to jump into a full peer-to-peer network model (*à la* Reed's Law) in which any combination of users may connect to any other combination of users in real time for any digitally-capable communication or collaboration, we are largely stuck with the network architectures, configurations, and policies that came before us. Consequently, at least in the near-term, we work with the network we have, not the network we want, and slowly morph to the network we want. For example, in a more ideal world, we would not have built out our telecommunications infrastructure with copper wire running across telephone poles, with limited-functioning end-user equipment, which predicated a network architecture characteristic of Metcalf's Law. Instead, we would have started with some combination of buried fiber and robust, well-apportioned wireless spectrum, and more versatile, upgradeable infrastructure and end-user equipment. Lawyers know this better than anyone as we safeguard the laws written by our predecessors and slowly steer the ship of state in, what we hope is, a better direction. We live and grow in a brownfield with existing structures and strictures.

This means we are stuck with legacy infrastructure and the current generation of power players, who may dictate how we connect and interact online for many years to come. This, however, does not mean that we cannot try to create large peer-to-peer networks without intermediating platforms. This also does not mean we should not try to morph the laws and policies to better enable user-empowered, peer-to-peer networking.

The next Sections of this Article explore opportunities for users to reclaim control over their content and data and, perhaps, establish better models for user-controlled data collaborations without the need for data intermediaries.

B. (Re)Rise of the User-Controlled Internet ... or then came Blockchain

i. Emerging Blockchain Technology, Architectures, and Processes and Potential Effect on Society … and Law

Back in the Winter of 2015-16 at the MIT Media Lab, Daniel "Dazza" Greenwood, a lawyer and data scientist, and I co-ran a month-long *Intensive Blockchain Rapid Prototyping Jam* in which students from MIT's Media Lab were tasked with deploying blockchain-based concepts to build new ventures and, in the process, disrupt a few industries and services, including the following: health care; financial services; content and media creation and distribution; hardware and software development; hotel management; invention control and licensing; real estate brokering and titling; art provenance; import/export services and other international supply chain tracking and processes; corporate governance; and citizen voting and other civic participation and government transparency issues. Students at the Brooklyn Law Incubator & Policy (BLIP) Clinic, which I created in 2008, provided the legal support to guide these prospective ventures down a legally viable path to disrupt existing non-blockchain-based services, products, and concepts.[43]

I am not generally one to view technology as the be-all and end-all solution to governmental regulatory oversight. These venture prototyping sessions at MIT to explore how to build blockchain-based competitive, disruptive services, however, made me rethink technocratic approaches, particularly with the unique power of blockchain technology to allow users to dis-intermediate trusted and untrusted governments, corporations, servers, and other brokers and intermediaries. blockchain concepts have the potential to allow every user, citizen, consumer, client, patient, creator, person to control all of their own assets – media, money, personal data – and to self-determine when and how and to whom and for when their assets may be utilized. That power might have the potential to be as revolutionary as any technological advancement humanity has ever known, at least until we realize the actual potentiality of artificial intelligence and quantum computing and whatever technologies might come afterwards.

Blockchain technology now has the potential to allow for micro-precise control over content and data flows. Blockchain technology should enable the originator of the content or the holder of personal data to self-determine if, when, how, to whom, and to what extent content or personal data is distributed and only for the purposes and duration for which the original person self-determines. All the relevant data associated with the content can be precisely measured, tracked, distributed, and retracted as the originator dictates in self-determined, self-executing "smart contracts." No third party would have the power to override the originator's determination of the desired use and flow

43. *Brooklyn Law Incubator & Policy Clinic*, BROOKLYN L. SCH., https://www.brooklaw.edu/Academics/Clinics%20and%20Externships/In-House%20Clinics/BLIP (last visited Mar. 13, 2024).

of the originator's media or data. This new-found precision in content control and flow is indeed revolutionary and gives the originators the control they had lost through both analog and digital copying and distribution revolutions. As far as I can assess, this is the most current realization of the true enabling power of digital technology and bespoke creation and distribution. Digital distribution, once the pariah of content owners or those who sanctify individual privacy and autonomy, might now be considered as the qualitatively best mechanism to preserve absolute control and distribution of content and individual data by the originator or owner of the content and data.

Blockchain technology enables a system in which data may be readily stored and secured at the edge and need not be centrally stored and processed. Until blockchain came along, many thought that data had to be centrally stored to maximize usability. This meant that data security had one single point of failure and vast amounts of data could be accessed simply by hacking one repository. Moving data storage and control away from central servers to millions/billions of edge points means fewer points of failure and means that data should be less susceptible to mass attacks and unwanted access. From a user perspective, blockchain opens the door to greater control and flexible, more precisely tailored data usage. Under traditional centralized server control by the data oligarchs (*e.g.*, Google, Facebook), the corporate data intermediaries only have access to, and control over, a narrow sector of the end user's data. Furthermore, these data controllers would not willingly combine their data to get a complete data picture of the end user. Additionally, the combined computational power of the unified end points is much more powerful than that of the central servers and clouds, making for much more robust algorithmic applications, while preserving data at each end point. Thus, end-user controlled blockchain-based networks could ultimately be far more robust and functional than the kluge network of multiple corporate data farms. Storing and securing data at user end points also opens up opportunities for each user to derive direct economic value — to get paid for each time the user offers its data or an entity requests the user's data.

ii. … And then came user/worker empowered organizing structures like "Platform Co-ops" and "DAOs"

Back around 2010, my BLIP students and I worked with a startup venture – Diaspora – four college students attempting to build a user-controlled, privacy-sanctifying, IP-securing social network, in which each end user would control their own user logs and only release their content, data, and other information when, to whom, for what duration and purpose as each user specifically self-determined.[44] This was before blockchain technology took root. Blockchain arguably makes this process of user data self-control and information flow significantly more viable. Diaspora's goal was nothing less

44. *See e.g.*, JIM DWYER, MORE AWESOME THAN MONEY, FOUR BOYS AND THEIR QUEST TO SAVE THE WORLD FROM FACEBOOK (Viking Press eds., 2014); Jim Dwyer, "*Diaspora is Real*", WIRED (Oct. 15, 2014, 12:00 AM), https://www.wired.com/2014/10/diaspora-is-real/.

than to revolutionize online social networks and to give full control to each user, but without the enabling power of blockchain technology and processes.[45]

The Diaspora founders were irritated that many social media networks owned a user's content, identity, data, user logs, and other personal information. The founders developed a privacy-aware, intellectual property-protecting, personally-controlled, open-source social network. The founders were the quintessential first-time entrepreneurs: they had a great idea but were unsure about how best to execute their vision. They were overwhelmed in a sea of corporate structure options, taxation issues, intellectual property concerns, and premature when it came to harnessing meaningful data protection technologies and systems. The existential conflict for these young entrepreneurs was that they wanted both to do *good* and to do *well* — they wanted to become a multi-billion-dollar venture and also pursue the public good. As such, they were conflicted about whether to become some sort of for-profit venture, a non-profit venture, some sort of hybrid social enterprise, or some sort of non-corporate entity. Diaspora was also the first entity to raise more than $200k on Kickstarter. The eyes of the world were upon them.

Others have made similar efforts to build user-centric social networks. These efforts have largely failed to take root and gain any viral uptake or network effects. But, across every iteration of the Internet and through the birth and mainstreaming of each transformative digital technology, some noble, enterprising, young entrepreneurs give it another shot, history be damned ... or are forgotten.

In any case, Diaspora – the intrepid, but perhaps pollyannish, and premature, startup – tried to establish its venture before such concepts as blockchain had become mainstream or even functionally possible. In recent years, there has been great optimism in disruptor and social entrepreneur circles that blockchain-based systems could be the key to user-empowered social networks. Add to that the coming of age of such concepts as "Distributed Autonomous Organizations ("DAOs"),"[46] "platform cooperatives,"[47] and other worker/user-controlled collectives and alliances.

---

45. The lack of functional blockchain storage and networking capabilities was not the only hurdle for our intrepid would-be disruptors and social entrepreneurs. There were preliminary corporate structure concerns. My students and I researched whether there were corporate structures that might enable the client to pursue both financial success and a broader public benefit agenda. The noble venturers ultimately chose a traditional Delaware C-Corp structure in the hope of enticing venture capital funding and to avoid legal uncertainty. The problem for this venture was that it failed to consider its revenue model, competing against other social networks (*e.g.*, Facebook) that could offer their services for "free" because they sold user data to third party marketing partners.

46. Distributed Autonomous Organizations are alliances built, owned, controlled by users without centralized ownership and management, typically using blockchain technology and processes for organization and governance. DAOs typically have no central governing body and the members have common goals and attempt to act in the best interest of the entity. In most jurisdictions DAOs are not (at least, not yet) recognized as officially corporate entities. *See What Is A Decentralized Autonomous Organization, And How Does A DAO Work?,* COINTELEGRAPH, https://cointelegraph.com/learn/what-is-a-dao (last visited Feb. 1, 2024).

47. Ownership in a cooperative is based on equity contribution or how much of the products or services the member purchases. Profits and earnings generated by the cooperative are distributed among

Diaspora had established itself as a C-Corp, but without an immediate revenue model (because it would not rely on selling user data or controlling the user experience). Platform Co-ops and DAOs and similar loose confederations of workers and users had not yet become mainstream, viable organizing structures.

Coming of age before the blockchain revolution, Diaspora relied only on the capabilities and functionality of "traditional" peer-to-peer networks. As a result, Diaspora and similar user-centric social networks failed to develop business structures or revenue models able to compete against the social network business model built on monetizing users and user data.

Now, we see the possibilities of DAOs and worker/user-controlled platforms in which the workers and users may share in the revenue derived from use of their data. Once again, many social entrepreneurs hope that these new organizing structures and data-control systems may break the stranglehold that the current cabal of Internet and social networking platforms have over exploitation of user data.

If Diaspora had organized itself as some sort of platform data collective, perhaps it would have been able to establish a recurring revenue stream derived from monetizing the collective user data (with the explicit consent of all the members of the collective). A next-generation social network, owned and controlled by its users as a cooperative could compete with the major social networking platforms.

By combining the enabling power of blockchain with the new-fangled user/worker-centric organizing structures like DAOs and platform co-ops, we have profound opportunities to give control of the Internet to the edge — to the users and workers. Digital technology is finally able to provide individual users, workers, user groups, and other communities and collaborations with the tools to organize and secure data online, and with those capabilities to allow users and user/worker groups to harvest the fruits of their data and/or

---

the members, or user-owners. People typically join a cooperative business to enjoy the benefits of group purchasing, pooled risk, and the empowerment of owning and controlling the company. Cooperatives differ from other forms of businesses because they operate more for the benefit of members than to earn profits for investors. All members are expected to participate and share the responsibility of running the organization. *See What is a Co-Op?,* NCBA CLUSA, https://ncbaclusa.coop/resources/what-is-a-co-op/ (last visited Jan. 21, 2024). A platform co-op is a co-op in which the co-op, itself, serves as the entity that offers the products, services, or content, where user members contribute and/or purchase the service. Platform co-ops may be owned and controlled by users, by workers, or by some broader communities of connected participants. Imagine Uber if the drivers owned and controlled the platform, or Door Dash if some combination of the local restaurants, the deliverers, and the consumers owned and controlled the platform. *See Platform Cooperatives*, UW CTR. FOR COOP., https://uwcc.wisc.edu/resources/platform-cooperatives/#:~:text=A%20platform%20co%2Dop%20is,skills%2C%20and%2For%20assets. (last visited Feb. 1, 2024). Perhaps, to the detriment of the attorney bar/guild, it would serve the broader community if states were to streamline the process to establish cooperative structures. Ventures and lawyers rarely think that a co-op is a viable corporate structure. If the process were streamlined, perhaps co-ops would be more of a default corporate structure.

labor — to claim the revenue derivable from use of their individual and/or collective data.[48]

Many in the blockchain space, have tried to deploy DAO structures for loosely organized governing and voting systems, but few seem to have deployed a DAO with any recognized, legally-recognized, corporate structure. Several states, Wyoming most prominently, have attempted to allow for recognized corporate structures, with consideration, of corporate responsibility and liability issues, but none of these statutorily-enabled structures seem to have taken root.[49]

iii. … And now come the Data Co-ops

Today, the ability to self-organize and empower user groups to control the flow and uses of their individual and collective data and labor is increasingly viable (arguably subject to certain jurisdictional approvals over corporate formation and liability) and could break the stranglehold of the Internet platforms and data brokers. But will we see new insurgent user/worker run collectives achieve critical mass and meaningful negotiating power to take the reins from, or at least match the power of the Internet network behemoths? Who will build the systems and structures to serve as the guarantors of individual and worker data autonomy in a world where our data is increasingly controlled by corporate powerbrokers?[50]

III. DATA INTERMEDIARIES, FIDUCIARIES, AND TRUSTMEDIARIES: FOURTH AMENDMENTS, THIRD PARTIES, SECOND CHANCES, AND FIRST PRINCIPLES

This Section considers the emergence of various flavors of digital intermediaries that may, to varying degrees, be authorized by users to handle

48. Fifteen years ago, I had suggested to the Skype leadership that they become the first online network to offer ownership and voting stakes to each of its members in lieu of an IPO or private sale. Skype could have become a globally-distributed and controlled organization — perhaps the first DAO before we even knew what a DAO was and before we had the blockchain technology to manifest a DAO. Now, such a concept, is increasingly more viable. Fifteen years ago, we were unsure of the process and consequences.

49. Casey Wagner, *Wyoming Passes Law To Give Daos A Nonprofit Legal Framework*, BLOCKWORKS (Mar. 8, 2024), https://blockworks.co/news/wyoming-non-profit-dao-legislation; Hope C, *U.S. State Wyoming's New Bill Gives DAOs Legal Existence*, YAHOO!FINANCE (Mar. 11, 2024), https://finance.yahoo.com/news/u-state-wyoming-bill-gives-044843295.html.

50. I served on the technology advisory committee for Eric Adams in his transition to become Mayor of New York City in 2021-22. It was my, perhaps naïve, hope that this incoming mayor might seize the moment and work to establish NYC as a protector or NYC residents' data against corporate and government exploitation. Mayor Adams had a fresh moment to enable NYC's residents to trust that their data would be secured and to even profit from use of their data and to self-determine when, where, how, and why corporate and government actors could use their data. Imagine NYC as a data trust, a data intermediary, a data fiduciary. I imagined a scenario in which NYC, on behalf of its residents, could build a platform and repository to store, encrypt, and secure the data of each NYC resident and to ensure that no other government or corporate actor could use, misuse, transmit, or exploit resident data without the explicit permission of the resident and without sharing the profits derived from resident data. This scenario has, to date, failed to gain traction.

user data in the best interests of the users and the obligations and benefits arising from such intermediary control.

A. The Common Law of Obligations: Trusts, Fiduciaries, and Bailors

A "trust" is a form of legal agreement that creates a legal entity where someone, or a number of people, serve as "trustee(s)" to hold property (and make decisions) for the benefit of specifically designated people or groups of people called the "beneficiaries." Each trustee has a legal obligation to make decisions with respect to the trust that are in the best interests of the beneficiaries. This type of obligation, called the "fiduciary" responsibility, may apply across relationships and professions, such that it may describe the duty a company's officers have to the company and shareholders, that certain financial advisors have to their clients, and that lawyers have to their clients. In general, a person acting as a fiduciary has a duty of care and a duty of loyalty toward those for whom the person is acting as a fiduciary. The duty of care requires a fiduciary to act reasonably in their decisions. An often-related duty of care imported from the common law of torts is the "do no harm" standard, which obligates the party not to impose physical or other harms on the other party. Meanwhile, the duty of loyalty perhaps indicates a higher standard of conduct that requires the fiduciary to act in the best interests of the other party (*i.e.*, the beneficiary. Legally binding on the fiduciary, these duties result in stronger protections and assurances for the beneficiaries involved. One of the most prominent components of the fiduciary duty of loyalty is to avoid a conflict of interest which prevents the fiduciary from using the beneficiary's information or assets to the beneficiary's detriment, the fiduciary's advantage, or both.

Another type of entity that relies upon the common law doctrine of obligations is the actual fiduciary. In modern society, these fiduciaries often are members of a profession, such as doctors, lawyers, and certain financial advisors, bound by their obligations pursuant to an explicit code of conduct.[51] Unlike the trust, these entities typically rely on contracts and other legal instruments to create and enforce formalized relationships with their clients or patrons.

A third type of obligation created at common law is bailment. Typically, this applies to individuals or entities (the "bailee") who have temporary possession of property on behalf of someone else (the "bailor").[52] Classic cases of the bailor-bailee relationship are the dry-cleaning business, and the parking valet at a restaurant. In each instance, the bailee warrants to the bailor that the property in question will be returned, at the agreed-upon time and location and in an agreed-upon condition.

---

51. Julia Kagan, *Fiduciary Definition: Examples and Why They Are Important*, INVESTOPEDIA (Sept. 25, 2023), https://www.investopedia.com/terms/f/fiduciary.asp.

52. BAILMENT, Black's Law Dictionary (11th ed. 2019).

A trust is advantageous because it frees up your time to pursue other ventures and activities, with the confidence that the trustee will work in your best interest. The trustee also likely has experience, data, and other insights from managing additional property. Pooled trusts, combined with expertise from handling multiple assets from numerous clients, may be extremely lucrative and have the potential to earn significant returns.[53]

The primary downside to using trusts is the cost, which is most often a percent-of-assets management fee or a fixed fee.[54] The fees can decrease as your assets under management decrease, while some trust funds charge higher fees on complex assets such as private equity investments, standalone businesses, or multigenerational parcels of land.[55]

In addition to the question of "how much to pay," there is a somewhat related question: to whom specifically do the duties attach? Fiduciary duties may be *assumed* due to an entity's consent, or automatically *imposed* due to "an entity's status, its specific role *vis-à-vis* its customers."[56] The latter category is easily seen in the relationships between lawyers and clients or doctors and patients.[57] On the other hand, voluntary assumption of fiduciary duties is often created by one party making external representations to another that the former will hold the sensitive information of the potential beneficiaries with care, loyalty, and other indicia of trust.[58]

Many of these trust-generating representations made by large technology platforms can be found in privacy policies and promises relating to data security, data minimization, and access rights.[59] However, there are few companies, entities, or associations that focus *primarily* on the manner of care and loyalty in which they or their constituents handle data – as a goal in and of itself – rather than using privacy as an incidental benefit to another primary service they offer.

---

53. *See, e.g., What is a Pooled Trust?*, NYSARC TRUST SERVICES, https://www.nysarctrustservices.org/nysarc-trusts/pooled-trusts (last visited Jan. 5, 2024, 6:24 PM); *CCT's Multiple Portfolio Investment Model*, COMMONWEALTH COMMUNITY TRUST, https://commonwealthcommunitytrust.org/medicare-set-aside/investment-information (last visited Jan. 5, 2024, 6:24 PM).

54. Amy Feldman, *Trust Costs Go Up; Get Ready to Negotiate*, BARRON'S: PENTA (Feb. 28, 2015), https://www.barrons.com/articles/SB51367578116875004693704580486391945783842.

55. *Id.*

56. Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L. J. 75, 90 (2020).

57. *id.*

58. *id.*

59. *See*, e.g., *Privacy Policy*, META (Dec. 27, 2023), https://www.facebook.com/policy.php; *Apple Privacy Policy*, APPLE (Dec. 22, 2022), https://www.apple.com/legal/privacy/en-ww/.

B. "Data" Trusts and Digital Fiduciaries

Data Trusts are "legal structures that give independent, third-party stewardship of data."[60] Data Trusts share many of the same characteristics as traditional trusts. For example, like a traditional trust, a Data Trust allows a trustee to make decisions about the corpus on behalf of the beneficiaries. In a Data Trust, these beneficiaries can include individuals, organizations, or essentially anyone or anything that holds data. Importantly, a Data Trustee, like a fiduciary, has a binding duty to do what is best for the beneficiary, much like a doctor has a fiduciary duty to do what is best for their patient, or a lawyer has a fiduciary duty to do what is best for their client. In other words, the trustee is not allowed to have a unilateral profit motive or, more broadly, a conflict of interest in the data or data rights under its custody. The key distinction is that Data Trusts are trusts in which the corpus of the trust is data, rather than real property, stocks, or bonds, and the decisions made concern that data.[61]

The key players in a Data Trust remain virtually unchanged from a traditional trust; however, the roles differ slightly. For instance, while settlors grant rights to trustees and trustees have fiduciary duties to beneficiaries, the beneficiary composition in a Data Trust may be expanded to those who are provided access to the data. For example, a data trust might determine that it would like its data to be used so that a hospital, a transit system, a municipal authority might want to harness the data to improve care or social services. These users of the data may be included among the beneficiaries of the Data Trust. Furthermore, Data Trusts can be particularly advantageous when there are conflicting interests between beneficiaries. A trustee can decide who may access and use the data under the trust's control. If that data user fails to comply with the terms and conditions, the trustee may revoke their access.

However, consider the competing interests of a corporation and consumers, or data subjects. If an entity that controls the data has a business interest in data provided by data subjects, this often results in a conflict between that interest and their duties towards data subjects.[62] Under these conditions, data controllers would be obligated to both maximize the value of the personal data they collect (for the benefit of shareholders) *and* honor fiduciary obligations towards data subjects.[63] The data subject, in some instances, may prefer that the data controller minimize the use, sharing, and monetization of its data. Therefore, a fiduciary obligation towards data subjects may be incompatible with the data controllers' responsibility towards

60. Peter Wells, *UK's First Data Trusts to Tackle Illegal Wildlife Trade and Food Waste*, OPEN DATA INST. (Jan. 31, 2019), https://theodi.org/article/uks-first-data-trusts-to-tackle-illegal-wildlife-trade-and-food-waste/.

61. Jack Hardinges, *What is a Data Trust?*, OPEN DATA INST. (July 10, 2018), https://theodi.org/article/what-is-a-data-trust/.

62. Sylvie Delacroix & Neil Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIV. L. 236 (2019), https://academic.oup.com/idpl/article/9/4/236/5579842.

63. *Id.* at 241.

shareholders.[64] Imagine a doctor who gains a commission on particular drug prescriptions or a lawyer who uses a company to provide medical reports for his clients while owning shares in that company.[65] In each case there exists a likelihood for a conflict of interest that brings into question whether the one under fiduciary duties is able to fulfill those duties to the extent the law requires.

While trusts as a legal structure have existed for centuries, Data Trusts are relatively novel. At present, there is no universal or standard model for Data Trusts, as each structure must be curated to address its unique circumstances and risks.[66]

The data fiduciary is still a novel concept at law. It should be clearly demarcated from a related but different framework articulated by Jack Balkin and Jonathan Zittrain known as the Information Fiduciary model.[67] The latter model posits that special relationships of trust and confidence arise between doctors, lawyers, or accountants and their customers not only due to legal contractual language, but also due to the exchange of sensitive personal information between the parties.[68]

An Information Fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship. People and organizations that have fiduciary duties arising from the use and exchange of information are information fiduciaries whether or not they also do other things on the client's behalf, like manage an estate or perform legal or medical services. Because most professional relationships are fiduciary relationships, most professionals are also information fiduciaries. And that means, in particular, that professionals have duties to use the information they obtain about their clients for the client's benefit and not to use the information to the client's disadvantage.[69]

Since online service platforms handle similarly sensitive data to lawyers and doctors, Balkin argues that such duties should extend to large online platforms.[70] Moreover, these fiduciary duties "run with the data" and do not require the formation of a specific contract between the individual and the data handler, easing the burden on individuals to use these platforms with reduced concern that their sensitive information is being mishandled.[71] Balkin posits that although these duties do not necessarily extend to advertisers that

64. *Id.*

65. *Id.*

66. A browser such as Mozilla's Firefox could serve as a technical extension of the trust/fiduciary, including having embedded duties of care/loyalty embedded in the code. But that would not obviate the need for a human being somewhere "in the loop."

67. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

68. *Id.* at 1207.

69. *Id.* at 1209.

70. *Id.* at 1221.

71. *Id.* at 1220.

leverage data, they should certainly extend to online service providers, "especially if you trust and depend on them."[72] For reasons of information asymmetries, user dependence, representations of expertise and good faith made by these platforms, and – most significantly – the potential for abuse, Balkin argues that fiduciary duties should be *imposed* by the government onto these platforms.[73]

On the other hand, Richard Whitt, a lawyer and policy advocate who has represented Internet platform providers and Internet disruptors for more than thirty years and who is currently a Fellow with the Mozilla Foundation and a Senior Fellow with the Georgetown Institute for Technology Law and Policy, argues that *voluntary* adoption of fiduciary duties by a willing entity is a more feasible and prudent approach.[74] After Balkin published the Information Fiduciary model, but before Whitt published his work, Lina Khan and David Pozen issued their own paper critiquing the Information Fiduciary model.[75] Similar to the arguments noted above, Khan and Pozen focus on the fiduciary duties that the directors of Facebook and Google owe to shareholders, and that the government mandated nature of the duty of loyalty attending the Information Fiduciary model would impede such duties by lowering the ability of Facebook or Google to monetize their data.[76] The mandated Information Fiduciary model would also risk violating the First Amendment.[77]

Whitt instead posits that the rich history of fiduciary obligations, rooted in the common law, can evolve just as common law doctrines do to apply to new digital applications.[78] Whitt discusses at length, not only the Information Fiduciary model noted above, but also the idea of what he terms a Digital Trustmediary. This Digital Trustmediary model "involves entities providing advanced digital service to their clients, while ***voluntarily*** operating under heightened fiduciary duties of loyalty, care, and confidentiality."[79] These Digital Trustmediary entities would arise from commercial contracts, codes of conduct, or other agreements between the user and the data handler.[80] Built upon *trust*, rather than on the technology,[81] the fiduciary's client would have an "actual understanding" of the fiduciary relationship,[82] thus allowing both parties to maximize the benefit of the relationship.

As noted above, a municipal authority could establish a Data Trust for its residents, through which data could be encrypted, secured, anonymized, pseudonymized, and used for any number of contractually authorized

72. *Id.*
73. *Id.* at 1222.
74. Whitt, *supra* note 53, at 90.
75. *Id.* at 79.
76. *Id.* at 84.
77. *Id.* at 85.
78. *Id.* at 101.
79. *Id.* at 76 (emphasis added).
80. *Id.* at 90.
81. *Id.* at 108.
82. *Id.* at 108.

purposes for the benefit of municipal residents and the municipality. Such data could be used to advance travel, police, health, education, and social services for targeted communities or the municipality more broadly.

C. Comparing Trusts and Contractual Fiduciary Duties

Fiduciary law in general offers the potential of providing protective measures to individuals who are too often left vulnerable online. This can be the case whether the individual is dealing with large tech companies or with smaller scale collaborative projects. Individuals may be forced to depend on services that accumulate and store personal data that may actually harm the data subject (*e.g.*, behavioral and targeted advertising).[83]

Applying trust law principles and practices to data may begin to remedy these situations. Under one scenario, for example, a legislative body could apply a statutory duty of care (reasonable conduct, do no harm standards) and bailment requirements (safekeeping of property interests standard) to any entity that collects and stores and shares personal data. By contrast, entities seeking to become data trusts or digital fiduciaries could adopt a higher-level duty of loyalty that runs with its beneficiaries. The ability to provide a higher level of protection to end user data opens the door to business models in which service providers could offer varying degrees of "privacy as a service" at varying costs.

Other proposals have recommended imposing fiduciary obligations on organizations that control data and rely on user trust.[84] Legislation introduced in the United States Senate has also put forth assigning fiduciary obligations on Internet Service Providers.[85] If enacted, such legislation could allow the Federal Trade Commission or state attorneys general to decide penalties for breaching these duties.[86]

Another approach for establishing fiduciary duties is through contractual obligations.[87] Traditionally, fiduciary duties were viewed as determining the course of action to suit the beneficiary through a general relationship-governance framework. This is in contrast to contracts, which spell out responsibilities of the parties before the relationship is formalized. Fiduciary duties offer some benefits for trusts; however, because some subscribe to the idea that a trust is a type of contract, the question remains as to whether trusts are distinct from ordinary contracts.

---

83. Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Heer Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

84. Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 499-500 (2019); s*ee also* Whitt, *supra* note 53, at 122–24 (describing the Data Care Act of 2018 and ACCESS Act of 2019).

85. Khan & Pozen, *supra* note 81, at 501.

86. *Id.* at 525.

87. Adam S. Hofri-Winogradow, *Contract, Trust, and Corporation: From Contrast to Convergence*, 102 IOWA L. REV. 1691 (2017).

For example, contract parties are able to equitably breach certain obligations while trust parties cannot.[88] While the contractual obligations of parties are bound by contract, even ironclad duties in trust law may be waived if a provision in a contract states as much. Furthermore, although trust fiduciaries are bound by the duties of loyalty and care, contract parties generally are bound only by good faith.

Some courts have recognized contractual fiduciary duties where (1) a duty of loyalty is not automatically invoked due to the nature of the fiduciary relationship and must be added contractually; or (2) non-fiduciary relationships where the parties wish to add a duty of loyalty. The former was introduced in *Gatz Properties, LLC v. Auriga Capital Corp.* (2012).[89]

D. The Data as Property Approach

Data has been deemed a new form of asset class by the World Economic Forum.[90] The major players in data collection and subsequent control are the well-known behemoths — Google, Meta, and the like.[91] Users, often ignorant of the economic value their data possesses, exchange their personal data with these entities for free services with no bargaining power.[92] Accordingly, users likely do not have any claim of ownership of their data as an asset, instead any potential ownership is transferred to the big Internet companies and possibly their majority shareholders.[93] From a property law lens, Data Co-ops could be a preferred mechanism for users to actually own their digital data-assets and maintain digital empowerment.

Legal scholarship has acknowledged that societal dependance on data calls for legal remedies that otherwise exist in property law. Though data is intangible, property law scholars James Grimmelmann and Christina Mulligan propose that an individual possesses data when they have control over at least one copy of said data.[94] The copy acts as the tangible piece of data protected by intellectual property law. Similarly, Jeffrey Ritter and Anna Mayer suggest that, since legal systems precisely define "goods," and include both agricultural

88. Taking the concept of unbreachable contracts a step further, in the context of blockchain-based "smart contracts", there is, generally, an encoded inability to breach the contracted provisions baked into the smart contract. *See infra* Part VI.

89. *Gatz Properties, LLC v. Auriga Capital Corp.*, 59 A.3d 1206 (Del. 2012) (holding that the LLC Agreement itself does not exculpate the controlling member-manager of the LLC and that the controlling member-manager violated a "contracted-for fiduciary duty by refusing to negotiate with a third-party bidder and by causing the company to be sold to himself at an unfair price in a flawed auction that the manager himself engineered.").

90. Beñat Bilbao-Osorio et al., *The Global Information Technology Report 2014 XI* (World Econ. For., 2014).

91. Michele Loi et al., *Towards Rawlsian 'Property-Owning Democracy' Through Personal Data Platform Cooperatives*, 26 CRITICAL REV. INT'L SOC. POL. PHIL. 769, 771 (2020).

92. *Id.* at 772.

93. *Id.* at 774.

94. James Grimmelmann & Christina Mulligan, *Data Property*, 72 AM. U. L. REV. 829 (2023).

commodities and manufactured products in such definitions, data could also fall into such categories.[95]

In the U.S. Uniform Commercial Code, goods are required to be "existing, identified, and movable at the time they are identified, in order for any interest in them to pass."[96] This definition of goods also includes the unborn offspring of animals and growing crops. Yet, it is the tangible born animal and the harvested crop that "becomes the asset around which a transaction is built."[97] Ritter and Mayer argue that data can be found to exist under a similar conceptual framework. They define data as "a record of an action taken, created and preserved in physical form, descriptive of an event, an action, a calculation, or the performance of a process."[98] As such a physical record, data could be governed under property law as a tangible good not unlike a harvested crop.

E. Co-ops, Platform Co-ops, and Data Co-ops

A "cooperative" is a business structure in which the users of the product or service are the members, owners, and operators of the company. More specifically, ownership in a cooperative is based on equity contribution or how much of the products or services the member purchases. Profits and earnings generated by the cooperative are distributed among the members. People typically join a cooperative business to enjoy the benefits of group purchasing, pooled risk, and the empowerment of owning and controlling the company. Cooperatives differ from other forms of businesses because they operate more for the benefit of members than to earn profits for investors. All members are expected to participate and share the responsibility of running the organization.

A "platform co-op" is a cooperative in which the co-op, itself, serves as the online, digital entity — a consortium of end users and related participants — that offers the products, services, or content, where user members contribute and/or purchase the service. Platform co-ops may be owned and controlled by users, by workers, or by some broader communities of connected participants. Imagine Uber if the drivers owned and controlled the platform, or DoorDash if some combination of local restaurants, deliverers, and consumers owned and controlled the platform.

Relying on these recognized forms of legal entity and organizing structures, individuals and groups of individuals, arguably with some minor government support through modifications of existing, statutorily-recognized corporate structures, trusts and co-ops may serve as viable vehicles to protect individuals' data in the digital age.

---

95. *Id.*

96. Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 221, 262 (2018)

97. *Id.*

98. *Id.*

By some corporate commercial interpretations, a Data Co-op is "a group organized for sharing pooled data from online consumers between two or more companies," in which the "members offer relevant marketing data gathered from browsing and purchases of online consumers in a jointly accessible data store."[99] This definition wreaks of a corporate-biased, (mis)identification of a Data Co-op and not what this Article intends to describe. Rather, a Data Co-op, for purposes of this Article, is a cooperatively-owned, democratically-governed group of individual end users who agree to safeguard and harness their data among themselves without a corporate service provider intermediary to which the end users relinquish their data. In this scenario, the data is not controlled by a third-party intermediary but by the user group. Essentially, it is a platform co-op in which the product is the end-user data, and the service is securing and harnessing that data for the benefit of the members of the co-op.[100]

Co-ops, by and large, are founded on communitarian principles and may seek to promote such values as democratic member control; solidarity; self-help and self-responsibility; member economic participation, equity, and equality; and autonomous and independent control, without control by outside organizations.[101] Co-ops also negate the need for intermediating service providers because the work is done by the members themselves. This certainly does not describe the type of commercial, corporate intermediary sometimes described as a "Data Co-op," even one that nobly services its end user customers or consumers.[102]

i. The Data Co-op as a Mechanism for Equitable Personal Data Management

Alex Pentland and Thomas Hardjono, MIT data scholars, compare the current data landscape to that of oil and big banks.[103] Standard Oil and J.P. Morgan were to the oil and banking industry what Google and Meta are to

99. Lori Paikin, *To Co-Op or Not to Co-Op?*, NAVISTONE (Oct. 2, 2019, 6:04:00 AM).

100. People could achieve a similar result with, perhaps, greater flexibility, by forming a Limited Liability Corporation granting either membership to those who contribute their data. The operating agreement could account for varying degrees of control for the members.

101. COINTELEGRAPH, *supra* note 44.

102. There is a half century long history, at least in America, of reclassifying "users" as "customers" or "consumers." It does seem strange that users of online services, even when not paying directly for those services or simply using an online platform are typically call "customers" or "consumers." This seems like an Orwellian NewSpeak effort to classify all online users less as participants and more as customers of -party online service providers. The co-op concept seems to reimbue and empower end users as *bona fide* participants in the online experience. Perhaps, an inverted Orwellian approach might be to adopt the library nomenclature of calling users of the library "patrons." Libraries think about their consumers/customers not even as mere "users." Libraries think of its users as citizens of the community — not citizens on a government list, but members of the community and people who are part of the civic infrastructure. Libraries do not see their patrons as a resource to exploit. Other service providers and the communities they service would be well advised to adopt a similar approach if their goal is to empower its participants.

103. Thomas Hardjono & Alex Pentland, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management* 2, MIT CONNECTION SCI. (May 15, 2019), https://arxiv.org/pdf/1905.08819.pdf.

data.[104] Their attempts to usurp near unilateral control in their respective fields threatened individual economic freedoms.[105] The solution to this threat, Pentland and Hardjono argue, was to establish trade unions and cooperative banking institutions to create a balance between the major entities and individual people.[106] Pentland and Hardjono suggest that, in the struggle against big tech for user data control, the modern equivalent to trade unions and bank cooperatives are Data Co-ops.[107]

A Data Co-op that allows users to pool data would effectively grant users the ability to gain an economic benefit from their own data without having to monetize it, but rather as a means to gain valuable insight via transparent analytics.[108] For example, major players in the ride-sharing sector (such as Uber and Lyft) do not provide mechanisms for drivers to compare their earnings for similar routes or distances. Likewise, passengers do not know how their fees compare to a similar ride another passenger has taken. A Data Co-op that pools this data would allow drivers and passengers to see whether they receive equitable payment or charges.[109] The utility of a Data Co-op in the context of medical and psychological care or municipal safety could offer even more profound benefits to the members of the Data Co-op and the broader community or municipality.

Nearly all credit unions manage their accounts through regional associations using common software. Accordingly, Pentland and Hardjono assert that "it is technically and legally straightforward to have credit unions hold copies of all their members' data, to safeguard their rights, represent them in negotiating how their data is used, to alert them to how they are being surveilled, and to audit the companies using their members' data."[110] However, as Pentland and Hardjono point out, while this may be true in theory, there has yet to be a test case of a credit union operating as a Data Co-op.[111]

Beyond an economic benefit, members of a Data Co-op would collectively have power over their data analytics and set democratic procedures to make collective choices regarding data governance.[112] Loi, Dehaye, and Hafen present Data Co-ops as touting the following essential features:

> a personal data management platform (PDMP) empowering individuals to collect, aggregate and control (copies of) their personal data from different sources (e.g., genomic data, e-health records, and e-commerce data), enabling clients to choose what data to share and with whom; and (B) democratic procedures that enable cooperative members to make collective

104. *Id.* at 2.
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. Thomas Hardjono et al., *Data Cooperatives: Digital Empowerment of Citizens and Workers 2*, MIT CONNECTION SCI. (Jan. 2, 2019), https://ide.mit.edu/sites/default/files/publications/Data-Cooperatives-final.pdf.
111. *Id.*
112. Loi et al., *supra* note 89, at 776.

> choices concerning: (a) general data analytics capabilities, policies and ethical codes for data transactions and services delivered through the PDMP; and (b) the deployment of surplus deriving from the secondary utilisation of data by third parties (e.g., for research, industry, or marketing purposes), once all costs associated with running the platform are deduced.[113]

Through these Data Co-op features, individual users are empowered to choose whether they want to share their data and can implement a democratic majority vote to set policies and ethical codes.[114] Accordingly, users would have the opportunity to control their own data assets, compared to relinquishing those assets to big tech.[115] Data Co-ops have the potential to "expand and equalise opportunities to control online choice architecture."[116] Unlike a dictatorial model where a single agent, or small group of agents, imposes rules for users, a Data Co-op offers a democratic model where co-op members can have greater autonomy in determining how their data is stored and used.[117]

As considered below, other data intermediaries, such as Data Trusts, would not provide all the benefits of the co-op model, which model serves to empower user groups, themselves, to safeguard their own individual and collective data and to self-determine the uses, and the scale and scope of such uses, of their data.

F. Differences Between Data Trusts and Data Co-ops

As discussed above, Data Trusts and Data Co-ops are two types of legal organizations that are designed to manage and control access to data. While they may seem similar on the surface, Data Trusts and Data Co-ops have several key differences. Data Trusts are legal structures that are used to manage and protect data on behalf of a group of stakeholders, while Data Do-ops are organizations that are, themselves, owned and controlled by their members.[118] In the Data Trust model, it is typical that an independent third-party entity acts as a custodian for the data and that a board of trustees have the responsibility for making decisions about how the data is used and shared.[119] Data Co-ops have many of the same goals as Data Trusts but diverge in management and control of data. In the Data Co-op model, members collectively decide how their data is used and shared.[120] Like a form of democratic governance, members have a direct say in decisions, thus resulting in a more equitable distribution of control and decision-making power over the data.

---

113. *Id.*
114. *Id.*
115. *Id.* at 778.
116. *Id.* at 782.
117. *Id.* at 779.
118. CREME GLOBAL, *What is a Data Trust? The Complete Guide for Organizations, Regulators and Manufacturers,* https://www.cremeglobal.com/what-is-a-data-trust-the-complete-guide-for-organizations-regulators-and-manufacturers/ (last visited Jan. 21, 2024).
119. *Id.*
120. Hardjono et al., *supra* note 107, at 2.

Data Co-ops and Data Trusts are both mechanisms for managing and utilizing large amounts of data on behalf of a group of individuals or organizations. While both have the potential to provide benefits such as increased security, privacy, and control over data, Data Co-ops are a superior model for data management because of factors like more control and higher transparency.[121] Specifically, the key advantages of Data Co-ops over Data Trusts include their democratic and participatory structure, transparency, control, and alignment with community values. In essence, Data Co-ops offer a more equitable and participatory approach to data management, ensuring that decisions are made in the best interests of all members.

Overall, Data Trusts function well in providing solutions for addressing the complex challenges of data management.[122] Data Co-ops, arguably, provide a better collective solution to a number of issues that arise in the use and implementation of Data Trusts and other similar data intermediaries. The first shortcoming of Data Trusts is the lack of member control. Governed by a board of trustees, data controlled by Data Trusts does not allow the individual stakeholder much, if any, control over how the data is used or managed.[123] Cooperative organizations, like the one proposed here, are owned and controlled by their members, who have a direct say in how the organization is run. The absence of member control, inherent to other data intermediaries, fundamentally limits the benefits of alternative data management schemes. Without adequate control, members may be unable to ensure that their data is being used in a manner that aligns with their interests and values, much in the same fashion as data controlled and exploited by corporations. Furthermore, a lack of member control contributes to a lack of transparency and accountability in data management.

A lack of transparency leads to the second shortcoming of other data intermediary models, the potential for conflicts of interest. Conflicts of interest arise when data managers priorities are not aligned with members. For example, some data intermediaries, such as data marketplaces, may be primarily focused on maximizing profits, rather than serving the needs of their members. This can lead to decisions that may not align with member interests. Turning specifically to Data Trusts, conflicts have the potential to arise because managers represent multiple stakeholders.[124] The first instance of potential conflict is between the trust and its beneficiaries. For example, the Data Trust may prioritize its own interests and goals by selling the data it holds to the highest bidder, regardless of the impact on the beneficiaries. The second source of potential conflict could be between data providers and data users when, for example, data providers want to restrict the use of their data, while data users may want access to more data. The final instances of conflict

121. *Id.*

122. *See* Kimberly A. Houser & John W. Bagby, *The Data Trust Solution to Data Sharing Problems*, 25 VAND. J. ENT. & TECH. L. 113 (2023).

123. *Id.* at 150.

124. *Id.* at 138.

happen between the trust and its service providers and regulators. Both service providers and government regulators might ask or demand the sharing of data, which may put the trust in conflict with its mandates and its beneficiaries' interests.

Ultimately, the hierarchical nature of Data Trusts deprives stakeholders of the democratic control that is integral to Data Co-ops, where members have a direct voice in the decision-making processes that impact their data.[125] Data Co-ops allow for a greater range of access. This is especially true for minority voices. The different governance structures ensure that members' voices are considered and aligned with the goals of the cooperative. In contrast, Data Trusts are usually managed by a small group of trusted individuals or organizations (trustees).[126] While trustees should consider the feelings and needs of its members, trustees ultimately rely on their own decision-making. The cooperative model circumvents the issue by giving its members direct decision-making control.

IV. WHEN THE GOVERNMENT GETS INVOLVED IN END-USER DATA ACCESS — LEGAL ORIGINS OF THE THIRD-PARTY DOCTRINE'S END RUN AROUND THE FOURTH AMENDMENT

The legal construct of the "Third-Party Doctrine" might provide the strongest argument as to why the Data Co-op, rather than the Data Trust or other intermediating fiduciary or bailee, would be the more secure and legally supportable vehicle to protect user data from unwanted third-party or government surveillance or misuse.[127]

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[128] This constitutional right shields citizens (if not all those within U.S. jurisdiction) against meritless governmental intrusion into their persons, houses, papers, and effects — essentially, individuals, their homes, their communications, and other possessions. The Third-Party Doctrine, however, holds that individuals who voluntarily provide information to a third party do

125. Katharine Miller, *Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data*, STAN. U. HUM.-CENTERED A.I. (Oct. 20, 2023), https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data.

126. Houser & Bagby, *supra* note 119, at 25.

127. The concept of the "Third-Party Doctrine" and the use of end-user data begs the question as to what happened to the "second-party": If the end user is the "first party," the Internet service provider is the "third party," who is the second party that should logically sit somewhere between the first and third parties? Is it the provider of the Internet access/transmission service connecting the end user to the Internet service provider (*e.g.*, the telecom or cable company)? The case law gives no insight. Perhaps there is an argument that the data fiduciary, be it a trust or co-op or other variety could serve as the "second-party" with heightened obligations to protect the data of the "first-party" above and beyond the obligations of the third-party Internet platform/service provider. No case law or articles address this concept, which could be fodder for a subsequent article.

128. U.S. Const. amend. IV.

not have a *reasonable expectation* of privacy[129] in such information.[130] Therefore, Fourth Amendment protections do not apply to information that is unwittingly and automatically shared with third party private entities such as Facebook, Google, Amazon, and Apple, enabling the government to seize and search it without probable cause or a search warrant.[131] All the government has to do is ask for it.[132]

The boundaries of the "Third-Party Doctrine" were outlined in *United States v. Miller* (1976)[133] and *Smith v. Maryland* (1979):[134] once an individual discloses information to a third-party, that individual forfeits any reasonable expectation of privacy they may have had in that information. In other words, the individual assumes the risk that this information may be revealed to law enforcement or some other government agency,[135] and there are no fiduciary duties of care and loyalty, or duties under bailment, or any other legal duties that can protect the individual's interest in their data. The Court in *Carpenter v. United States*[136] might have laid the groundwork to allow vehicles like the Data Co-op to protect end-user data from unwanted surveillance and use.

Decades after *Miller* and *Smith*, in *Carpenter v. United States*, the FBI obtained 12,898 cell-site location information ("CSLI") points cataloguing Carpenter's movements over 127 days, which showed he was near four robbery locations at the time those robberies occurred.[137] The Court held that when the government accessed CSLI from the wireless carriers, it "invaded Carpenter's reasonable expectation of privacy in the whole of his physical

129. Arising in the John Marshall Harlan concurrence in Katz, the "reasonably expectation of privacy" became the *de facto* standard for Fourth Amendment claims following the Court's decision in 1967. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

130. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

131. RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 20 (2014). State laws can provide more rights than federal laws. The Third-Party Doctrine is a constitutional floor, meaning states can limit its application via statute and provide more rights to its residents.

132. *Id.* at 1. There is an additional issue that eviscerates protection of user data from government surveillance. The courts essentially treat one's mobile phone is a "place" subject to deference under "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. The courts, however, do not treat use of one's face or fingerprint to access one's phone as protected "testimony."Thus, one's face or fingerprints are not protected as speech and not protected against the right of self-incrimination under the Fifth Amendment. As a result, law enforcement may simply require you to press your finger on a phone or look into your camera to break privacy without a warrant and without implicating the First, Fourth, or Fifth Amendments. In lieu of facial or fingerprint access (which the courts, arguably incorrectly, characterize as non-testimonial, we could design a system that would require "testimony" for access. For example, to access one's device, the user might have to answer questions such as "tell me with whom did you slept last night and what did you write about them in your journal," or "what item did you steal from the office supply closet last week". The right against self-incrimination would protect the user from answering. It might be as simple as creating a skin that converts one's phone into a private diary.

133. United States v. Miller, 425 U.S. 435, 443–44 (1976).

134. Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

135. *Id.* at 744.

136. Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018).

137. *Id.*

movements."[138] The Court relied on *Katz v. United States*, which held that a person has a "reasonable expectation of privacy" protected by the Fourth Amendment when making a phone call from a telephone booth.[139] The Court recognized a qualitative difference between the "limited types of personal information addressed in *Smith* and *Miller*, and the exhaustive chronicle of location information casually collected by wireless carriers today."[140]

According to the Court, collecting and tracking CSLI is more akin to the facts of *United States v. Jones*, where the government's installation of a GPS device on the defendant's car and its use of that device to monitor the vehicles' movements constituted a search within the meaning of the Fourth Amendment.[141] CSLI, like GPS tracking, allows the government to "chronicle a person's past movements" through "detailed, encyclopedic, and effortlessly compiled" cell phone location information.[142] These tracking tools are more cost-effective and easier to implement than other traditional investigative methods, and they reveal "not only particular movements, but... familial, political, professional, religious, and sexual associations."[143] The difference is that CSLI is even more invasive on an individual's privacy than GPS tracking because people carry cell phones on their person at all times, "beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[144]

The retrospective feature of CSLI also made the Court hesitant to allow police to freely access it, effectively "travel[ling] back in time to retrace a person's whereabouts ... for up to five years."[145] The automatic and continuous recording of CSLI for every person, not just those under police investigation, would provide police with the power to track anyone without even knowing in advance whether they want to follow them.[146] The Court saw this as affording police too much ability in circumventing Fourth Amendment protections.[147]

The dissent by Justice Gorsuch in *Carpenter* presents a logical argument that user digital data, particularly when the user has expressly and affirmatively demonstrated a desire to protect their data privacy, should not be tainted by the Third-Party Doctrine. Perhaps a privacy-intentional vehicle like a Data Co-op should be sufficient to protect user data from application of the Third-Party Doctrine.

---

138. *Id.* at 2219.

139. Katz v. United States, 389 U.S. 347, 360 (1967).

140. *Carpenter*, 138 S. Ct. at 2219. CSLI is much more personally revealing in nature than call logs and bank statements. *See Id.* at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breaths, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that it is collected by a third party does not make it any less deserving of Fourth Amendment protection.").

141. *Id.* at 2216.

142. *Id.* "A phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 2217.

143. *Id.* at 2217–18.

144. *Id.* at 2218.

145. *Id.*

146. *Id.*

147. *Id.*

Gorsuch's dissenting opinion in *Carpenter* expressed skepticism with respect to the Third-Party Doctrine's ability to survive in the modern digital age.[148] He noted that most Internet companies "maintain records about us and, increasingly, for us."[149] In the past, these records, including private information, would have been locked away or destroyed but now exist in potential perpetuity on third-party servers.[150] The Third-Party Doctrine assumes that no one reasonably expects any of this information to be kept private, but in reality, most people *do* expect that information they give to third parties will be kept confidential.[151] He noted the Fourth Amendment provides protection of your "persons, houses, papers and effects, against unreasonable searches and seizures" and in some circumstances the data you entrust to Internet companies can be considered "modern-day papers and effects," entitled to the same level of protection.[152] CSLI is also "customer proprietary network information," which carriers may not disclose without the customer's consent.[153] Gorsuch contemplated that, because customers have "substantial legal interest" in their CSLI, "including at least some right to include, exclude, and control its use," these interests may even be deemed a property right.[154] Gorsuch suggested that Carpenter could have prevailed on a trespass test used in *United States v. Jones* and *Florida v. Jardines*.[155]

There is a stark difference between consenting to allow a third party access to your property and consenting to allow the government to search that property.[156] Gorsuch described entrusting your property to Internet companies as a bailment, which is "the delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose."[157] As noted above, bailees owe a legal duty to protect property.[158] He observed, "just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections."[159]

Ultimately, Gorsuch agreed with the majority's decision but disagreed with the majority's reasoning. Gorsuch agreed that law enforcement agencies need a warrant to access cell phone data, but rather than applying the *Katz* reasonable expectation of privacy test, Gorsuch reasoned that CSLI records

148. *Id.* at 2262.

149. *Id.*

150. *Id.* at 2261–62.

151. *Id.* at 2263 ("People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private.").

152. *Id.* at 2269.

153. *Id.* at 2272.

154. *Id.*

155. *Id.* at 2265.

156. *Id.* at 2263. "The fact that a third party has access or possession of your papers and effects does not necessarily eliminate your interest in them." *Id.* at 2268.

157. *Id.* at 2268 ("Entrusting your stuff to others is a bailment.").

158. *Id.* at 2268-69 ("A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the 'implications from their conduct' if they don't.").

159. *Id.* at 2270.

are the property of the cellphone owners, and, under the Fourth Amendment, law enforcement agencies cannot search a person's property without a warrant. For the government to secure a timely and reasonable warrant, it would need to articulate probable cause to search and restrict the search to a reasonable timeframe instead of obtaining access to all available records. If law enforcement is capable of obtaining a warrant, companies must comply with the request.

The law has evolved substantially to give effect to certain principles regarding the collection and use of data. For example, Europe's General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act ("CCPA"), and the California Privacy Rights Act all enforce permutations of certain concepts such as notice, choice, transparency, and consent. These laws give control back to users over their data. And yet the Third-Party Doctrine eviscerates any fair interpretation of these fundamental concepts because it involves purely *ex parte* negotiations and communications between private technology companies and the state. Thus, all these laws do from a law-enforcement access standing point is allow companies to place hard-to-find representations of "good faith" efforts in their privacy policies to avoid potential liability.[160]

There are a few examples outside the context of privacy policies where companies affirmatively display and represent to consumers an intent to provide certain rights. Many of these representations are the product of privacy legislation. For example, under the CCPA, websites must have a page called "Do Not Sell My Personal Information," which allows consumers to opt-out of the sale of personal information. Meanwhile, other efforts are actually made in response to *avoid* legal requirements. For example, "warrant canaries" are voluntary notices on a company's website that state that a company has *not* complied with a government data access request under, for example, the Foreign Intelligence Surveillance Act,[161] in a certain number of days.[162] Usually, when the government orders the production of information from a technology company through a subpoena, there is a corresponding gag order.[163] Warrant canaries are industry efforts to toe the line of the law and explain to their consumers that the company has, in fact, disclosed its customers' information.

Alternatively, a new approach could combine common-law property rights with the *Katz* reasonable expectation of privacy test. In property law, individuals tend to have a greater expectation of privacy in both real and personal property that belongs to them. When applied to data collected and held by an organization, the question becomes: what kind of legal interest is sufficient to make something *yours*?

160. *See Privacy Policy*, META (Dec. 27, 2023), https://www.facebook.com/policy.php.

161. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-85(c).

162. Kurt Opsahl, *Warrant Canary Frequently Asked Questions*, ELEC. FRONTIER FOUND. (Apr. 10, 2014), https://www.eff.org/deeplinks/2014/04/warrant-canary-faq.

163. *Id.*

Complete ownership or exclusive control may not be necessary to assert one's Fourth Amendment rights. As noted above, because the nature of data is not well-determined under law, it is also conceivable that ordinary property law is insufficient to cover the potential harms from breaching fiduciary duties. For instance, even paying for an Uber, hotel room, or telephone booth has produced a license to use or control a space temporarily.[164]

There are a several options available for Internet companies seeking to become data fiduciaries and to better protect the interests of their patrons. As noted above, while the prescriptive imposition of legislation is unecessary, given the voluntary nature of the entrustor-entrustee relationship, legislative bodies could pass laws to create powerful incentives for entities to become data fiduciaries.[165] Entities on their own could also adopt and implement best practices, codes of conduct, or self-certification regimes.[166]

Another path is creating an entirely new profession for digital agents. Much like a physician or an attorney, the digital fiduciary agent could hold itself out as a member of a professional guild of experts. As Whitt notes, treating a digital "trustmediary" as its own profession, complete with enforceable codes of conduct and disciplinary processes, also "can qualify for special treatment under the U.S. Constitution."[167] Mike Godwin, along with many other Internet legal theorists, have argued that such entities should have legal standing to defend their clients' Fourth Amendment rights against government searches and seizures.[168] To the extent that analysis, buttressed here, proves correct, "a professional [Digital Trustmediary] becomes all the more attractive to would-be clients."[169]

Exactly how this road to the Fourth Amendment fiduciary plays out in the near term is unclear. Perhaps there are opportunities for the state or for gilded professional consortia to license such fiduciaries and to regulate their conduct, similar to lawyers and doctors, that abides by the common law of obligations and acts under a code of conduct that *voluntarily* imposes fiduciary duties to the handling and disclosure of users' data. Professional fiduciaries of this kind typically use contracts to formalize the fiduciary relationship with their clients.

Lawyers are obligated to safeguard client funds and information and to preserve client confidentiality. Tacking on an explicit role for state barred lawyers to function as data fiduciaries is hardly a stretch for forward-looking state bar associations to explore.

---

164. *See, e.g.,* Engblom v. Carey, 677 F.2d 957, 963 (2d Cir. 1982) (holding that quartering state-controlled National Guard soldiers in homes during peacetime violated tenants' Third Amendment rights).

165. *See, e.g.,* Bennett Cyphers & Cory Doctorow, *The New ACCESS Act Is a Good Start. Here's How to Make Sure it Delivers.*, ELEC. FRONTIER FOUND. (June 21, 2021), https://www.eff.org/deeplinks/2021/06/new-access-act-good-start-heres-how-make-sure-it-delivers.

166. Whitt, *supra* note 54, at 124.

167. *Id.* at 125.

168. *Id.*

169. *Id.*

Alternatively, an Internet company could use its terms of service and privacy policy to act as a contract that spells out the nature of the fiduciary relationship. Too often, though, the average consumer will not read the privacy policy or terms of service. Another option could be for the company to post a seal or similar watermark on its website, app, or marketing materials that would signal to consumers the approach the company will take when handling data access requests from law enforcement. A consortium of companies could share a common Certification Mark to indicate that they abide by a set of standards that sanctify user data or at least offer a set of heightened protections to safeguard and limit the redistribution of user data. That consortium of companies could enter into a Global Memorandum of Understanding memorializing a set of best practices to which these good actors would adhere. Or an international Standard could be adopted by the Institute of Electrical and Electronics Engineers ("IEEE") or other globally-recognized organization.

Regardless of how the fiduciary relationship is formed and instantiated, the larger conclusion remains. The digital trustmediary should be able to act on behalf of its clients and patrons, as the "constitutional floor below which Fourth Amendment rights may not descend."[170]

Data Trusts may serve to fill the gap in constitutional protection that currently exists over personal data shared with third parties. Those entities voluntarily seeking to act as fiduciaries with their patrons' personal data should be able to "stand in the shoes" of their patrons and only provide any sensitive (and potentially incriminating) information to law enforcement through a transparent, structured, and standard-based process.

Data Co-ops, however, arguably offer even stronger protection against government access to user data shared with third parties. Arguably, Data Co-ops cut out the middleman, the third-party intermediary. As such, the data is controlled directly by end users without any intermediaries, through which the end user might have disavowed the end user's privacy interest.

There are inherent problems with relying on anything or anyone that looks like an intermediary if the goal is to guarantee privacy as a technological matter and as a legal construct. This is true even with trusted intermediaries with heightened obligations to its end users. This is arguably true even with Data Co-ops, which may or may not be deemed as third-party intermediaries or as the end-users themselves.

There is an argument that the creation of a Data Co-op keeps all the data within the control of the "first-party," *i.e.*, the data is never given over to a third-party and, therefore, the user(s) have not abandoned their privacy interest.[171] If this were the case, government could not access the data without a properly issued judicial warrant. It is conceivable that a state authority could provide a

170. *Id.* at 129.

171. To the extent that we view corporations as first-party entities, even to the extent we view biological ecosystems as single entities (*e.g.*, coral reefs), we certainly could view data conglomerates as a single unified entity with first-party rights.

secure Data Co-op model to its own citizens and residents to protect against the federal government's request for end user data. Why might this be a public benefit to the state's and its citizen's interests? With a patchwork of disparate federal and state laws on such issues as abortion, cannabis, and gun ownership, it is conceivable that a state might want to protect its citizen's state rights against encroachment by the Federal government or another state. In the wake of the Supreme Court Opinion in *Dobbs*,[172] a state might want to ensure that data about a person crossing a state line for an abortion or IVF treatment is not easily shared with other states or the Federal government with a goal that runs counter to state policy on abortion rights or embryo status and personhood. A similar argument could be raised in the context of a state that has cannabis laws that run counter to federal law or laws of a state seeking data on one of its residents who left the state to acquire cannabis.

Thus, perhaps a state or a municipality could set up a state-approved public data fiduciary, trust, or co-op for its residents to protect data from external government (or corporate) access and use of resident data.

V. PROBLEMS WITH THE APPLICATION OF INTERMEDIATING TRUSTS/FIDUCIARIES

There are various problems in relying on intermediaries, even trusted intermediaries, with heightened obligations to their end users. In particular, applying any legal concept or law becomes increasingly untenable when applying law across jurisdictions, which is inevitable in the case of online data controllers. This is particularly problematic given that all online communities obliterate geo-political boundaries, and any data intermediary could be subject to the disparate laws of multiple jurisdictions. Regardless of what approach or model we take to establish a method to protect user data, we will have to confront multiple hurdles. Some are considered below.

In a traditional Trust Model, it is important to reiterate that because data is not automatically considered property under U.S. law, there is concern that litigation could render this model untenable.

In a contractual framework model, in which the terms of the data trust are simply reduced to writing, there are the advantages of flexibility and adaptation, with changes being as simple as amending the contract. However, this has the downside of limiting participation to those who have signed the agreement, and every new party looking to access the data would need to contract with each data provider. Covering the scope of an ongoing data trust via contract would be difficult and could quickly become a clerical mess.

In a corporate structure model, a separate entity would be created to manage and provide access to the data. This could be via a separate entity, a partnership, a Limited Liability Partnership (LLP), an LLC, a corporation, or other legally-recognized business structure. By using a traditional corporate

172. *Dobbs*, *supra* note 1.

form, data providers could license data to the corporation, and representatives of the data holders or an independent body could act as a board. Data providers could be the "shareholders" under this model. LLPs could also be considered due to the limitation of liability in the event the collaborative becomes insolvent, or a claim is made against it. The structure of an LLP makes it more suitable for smaller collaborative efforts due to its governing structure, where each member typically has equal decision-making power. While other options, such as charity organizations or unincorporated entities, including distributed autonomous organizations ("DAOs"), exist, they have several drawbacks that make the previously mentioned governance structures more suitable.

In any case, the entity must be incorporated in some acceptable form and within some amenable jurisdiction. Which jurisdictions have advantages or disadvantages for data trusts would depend on a few factors, including: size, scope, and scale of the trust; purpose of the trust; future expansion ideas; tax implications; etc. Such an analysis could be undertaken in the future if this option were chosen. That being said, the applicable law being analyzed would depend greatly on the type of data being held in the data trust. For example, assuming the data trust contained personally identifiable information ("PII") of European and American individuals, privacy laws of each jurisdiction would have to be researched to ensure compliance. For the former, the GDPR and any country-specific law that might heighten the requirements would need to be examined. For the latter, the type of data would dictate if there were any federal regulations, while any state law may govern if federal law does not.[173] The increasing patchwork framework of U.S. state laws would further complicate addressing privacy matters. In addition, the interplay between these systems would be examined. For example, for the GDPR to be satisfied, U.S. data would have to be protected according to the GDPR standards.

There are also serious potential problems in the event of sale, acquisition, merger, bankruptcy, or dissolution of the data intermediary. Who controls the data, and to what extent do the data control obligations apply in the context of an acquired, merged, bankrupt, or dissolved entity?

With regard to government access to user data in the context of data intermediaries, the law is still variable across global jurisdictions and will likely remain uncertain for many years. As such, users are at the whims of judicial interpretations of the Third-Party Doctrine and the scope of the Fourth Amendment to user data. Users are also subject to varying, perhaps arbitrary, determinations by the data intermediary regarding whether and to what extent to comply with a government request for user data.

---

173. U.S. privacy laws are particularly fractured. The applicable law is dependent on the type of data, for example health information is handled under the Health Information Portability Accountability Act ("HIPAA"). Several other types of data are subject to different federal entities, while state law can vary on not only privacy laws but data breach laws. *See* Müge Fazlioglu, *Filling The Void? The 2023 State Privacy Laws And Consumer Health Data*, IAPP (Mar. 28, 2023), https://iapp.org/news/a/filling-the-void-the-2023-state-privacy-laws-and-consumer-health-data/.

VI. DATA CO-OPS, ALGORITHMS, AND VIRTUOUS USE OF INDIVIDUAL AND AGGREGATED DATA

There is great potential to use private or public Data Co-ops to simultaneously protect the privacy interests of the co-op members while allowing broad use of the member data to advance the interests of the members. For example, it seems quite plausible for a community—even a state or municipal authority—to create a Data Co-op specifically designed to safeguard and harness for the good of the group the individual and aggregated data of the community small or large. Perhaps it is too grand a starting point, and too tenuous an argument to avoid Federal government invocation of the Third-Party Doctrine, for a state or even just a municipality (*e.g.*, San Francisco or New York City) to establish a public data fiduciary, trust, or co-op to protect its residents. The Third-Party Doctrine's end run around the Fourth Amendment is more likely to apply and to allow government access to end user data even when an intermediating Data Fiduciary explicitly commits to safeguard end user data than when the end users, themselves, directly control their data individually or within their own co-operative. As such, perhaps the better approach to pave the way for user data protection would be for SF or NYC resident groups to create their own Data Co-op testbeds to prove out the concept. Perhaps the New York City Municipal Credit Union could establish itself as a Data Co-op to secure the data of its members and to use that data only for purposes agreed upon by the members and users of the Credit Union.[174]

In addition to securing resident data, such a Data Co-op could advance any smart city initiatives NYC might deploy. Each member of the Co-op could deposit their data with the Co-op. Each individual would be able to participate in aggregated data usage to build algorithms that would enable the Co-op to understand how to build a more functional city or community. If our health data, financial data, travel data were secure but accessible for algorithmic interpretation, imagine how we could improve city services and processes. Historically, it seemed technologically untenable to build such a trustworthy, secure system. It now seems like we could join the enabling powers of blockchain technology and platform co-ops to build a functional Data Co-op for the betterment of the community without sacrificing individual privacy.

Perhaps even the NYC Municipal Credit Union is too big an entity for the first experiments in user-protecting, community-enhancing Data Co-ops. There are smaller communities, like hospitals or schools, community boards or business improvement districts, that could serve as viable testbeds through which the community could harness data from a large community, without compromising individual data, to better serve the needs of the community through better analysis, synthesis, and application of medical data to help the

174. HARDJONO ET AL., *supra* note 110.

members individually. At least hospitals and schools are statutorily and regulatorily bound by heightened obligations to secure user data.

The easiest path to establish a functional, useful Data Co-op might be simply to tap into existing co-ops (*e.g.*, telecom cooperatives; Wi-Fi mesh networks; energy user cooperatives; farmer co-op; worker co-ops), which already have cooperative mindsets and a commitment to sharing. Such user cooperatives could expand their mandate to collect user data, to encrypt and to anonymize the data, and to use the data for whatever purposes dictated by the understanding between and among the co-op members. They could even license out the data to third-party data exchanges or aggregators or other data-hungry third parties, if allowed and pursuant to the co-op rules. The rules governing use of data, both individualized and aggregated, could be as broadly, as narrowly, or as mutably defined as the co-op rules provide. This is where blockchain becomes a useful tool by allowing for automated smart contracts that could precisely tailor where, when, how, to whom, for how long, for what purpose, and for what economic or social purpose the mutually agreed upon algorithm dictates or triggers.

These Data Co-ops could even be set up as multistakeholder cooperatives, in which parties other than the data providers could have a stake (*e.g.*, subject matter experts, public health officials, school administrators, transit and urban designers) if agreed upon by the co-op members.

When the Supreme Court issued its opinion in *Dobbs*,[175] abortion-rights activists were quick to warn of the consequences of weak privacy protections in health apps. With increased surveillance comes an increase in risk of criminal liability—both for people seeking abortions and abortion providers.

Many people use period-tracking apps, which could store health data about when someone missed their period. Other people may text their friends about needing abortion resources. Meanwhile, many people utilize their digital map apps to locate health clinics. While these resources are generally helpful, they can expose a person to potential liability in a state where abortion is unlawful or even illegal. Furthermore, tech intermediaries must comply with law enforcement requests for information under statutory and constitutional laws.

As defined by HIPAA, protected health information ("PHI") is "the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care."[176] However, what happens when health information is not collected by a healthcare professional? There are currently no federal laws to specifically regulate health data collection outside of the healthcare provider

175. *Dobbs*, *supra* note 1.

176. Ben Lutkevich, *Definition: Protected Health Information (PHI) or Personal Health Information,* TECHTARGET, https://www.techtarget.com/searchhealthit/definition/personal-health-information#:~:text=Protected%20health%20information%20(PHI)%2C,an%20individual%20and%20determine%20appropriate (last visited Mar. 13, 2024).

context. What does this mean for consumers of health apps? Currently, only five states—California, Colorado, Connecticut, Utah, and Virginia—-have enacted comprehensive consumer data privacy laws. Even these data privacy laws burden the consumer with asking the business what it does with their private data, and specially requesting that they delete it.

Existing US state privacy laws generally provide the following:

- The right to know about the personal information a business collects and how it's used and shared;
- The right to delete personal information collected from them;
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their privacy rights.

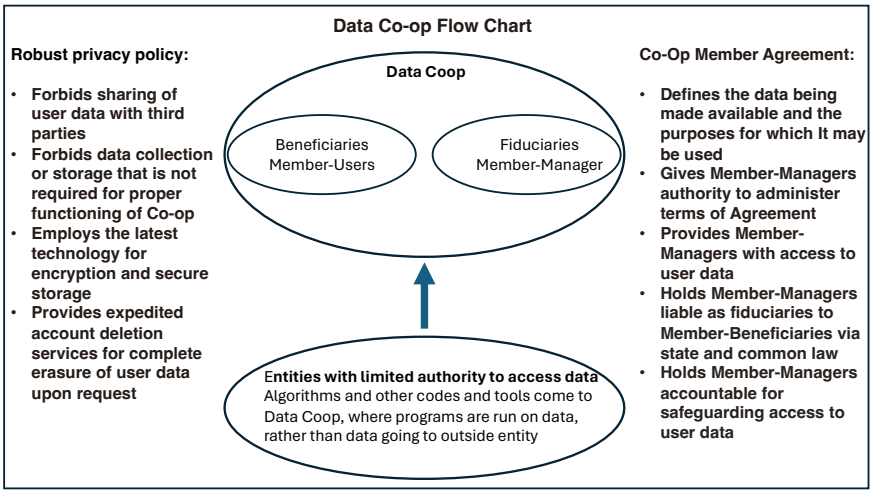
Two problems emerge: (1) This is not a universal federal standard; and (2) it places a burden on users to go out of their way when it comes to safeguarding highly personal information—such as health data.

Nearly a third of women in the U.S. use a period tracker, and data privacy is not guaranteed.[177] There is no prevalent one-stop-shop for them to track their cycles and get the products they need, all in one place. Every month, these consumers must be conscious of the fact that they may need to purchase more products.

Since *Dobbs*, my students in the Brooklyn Law Incubator & Policy (BLIP) Clinic and I have been working to build MNTHLY—a Menstrual Cycle Tracking application—to ensure that sensitive user data is always secured and protected and sanctified as private end-user data, not available to any third-parties or government. Our concern was the ability for state actors to view and analyze data and to determine that the user is pregnant and might seek abortion services, perhaps even traveling across state lines for such services, in possible violation of a state's anti-abortion laws. We are attempting to build this application with technology that would allow all data to reside as close as possible to the end-user, either on the end-user's own device or server or within a locally cached server to which no third-party would have access. To the extent the data is to be run through any algorithms, *the algorithms would come to the data* rather than having the data go to the algorithm on some external server.

177. Eva Epker, *Survey Finds Women's Health Apps Are Among The Least Trusted: What To Know And How To Keep Your Data As Safe As Possible*, FORBES (May 16, 2023, 4:11PM EDT), https://www.forbes.com/sites/evaepker/2023/05/16/survey-says-womens-health-apps-are-among-the-least-trusted-what-to-know-and-how-to-keep-your-data-as-safe-as-possible/?sh=1a398dec68b8 (citing *Health Apps and Information Survey,* KAISER FAM. FOUND. (Sept. 10, 2019), https://www.kff.org/other/poll-finding/kff-health-apps-and-information-survey/).

We debated whether a Data Trust[178] or a Data Co-op model would work better for MNTHLY. Logistically, the Data Trust seemed more manageable, because it would simply require the hiring of a professional fiduciary to run the Data Trust, without having to involve the members directly. We, however, concluded that a Data Co-op would arguably protect the data better, at least from government actors hoping to use the Third-Party Doctrine to access member data. Thus, the Data Co-op model seemed to be the best model to ensure the data does not fall into the hands of any third-party intermediary or the government. Such a model would help to ensure the user's privacy to the fullest extent possible and would also ensure such related rights as the right to travel, particularly across state lines without the specter of corporate or government surveillance. Below is a chart depicting a possible approach such a Data Co-op, or Data Trust if deemed sufficiently protective of data against third-party and government access, could follow:



179

There are still technical hurdles to overcome, particularly with regard to anonymizing, pseudonymizing, and de-identifying users, as well as limiting the scope of the data usage for its precise, targeted goals and durations; but, from a legal perspective, the data protection issues become easier to appreciate, respect, and control.[180]

178. Another path the BLIP Clinic has explored is working with a hospital or doctors' collective to create a HIPAA-compliant data trust. All data would be held in a doctor-run repository and could not be released without explicit approval. This would add an extra layer of medical privacy protection above and beyond any protection offered through the data trust structure.

179. This chart also works to describe a Data Trust model (simply swap out "Members" with "Trust" and "Co-op Agreement" with "Trust Agreement").

180. Dept' of Health and Hum. Serv. Subcomm. on Priv., Confidentiality & Security, Nat'l Comm. on Vital and Health Stat., *Transcript of the Subcommittee on Privacy, Confidentiality & Security Hearing on De-Identification and the Health Insurance Portability and Accountability Act (HIPAA) Panel III: Approaches for De-Identifying and Re-Identifying Data* (May 25, 2016), *https://ncvhs.hhs.gov/transcripts-minutes/transcript-of-the-may-25-2016-ncvhs-subcommittee-on-privacy-confidentiality-security-hearing/*;

VII. SOME HURDLES AND QUESTIONS TO CONSIDER WHEN FORMING A DATA CO-OP

While Data Co-ops may pose the best model to secure and monetize user data for the maximum value to end users and end-user groups, there are some lingering questions to address and to resolve depending on the location of members, types of members, and member preferences within a data collaborative. Among these issues are the following:

1. What is the process for handling security breaches in the database if they occur? What are the implications if a specific member's mishandling of data is the reason for data hack? What if a member does not mishandle data but is still hacked, should it still be responsible for damages?
2. Many jurisdictions have data breach laws dictating who needs to be notified in the event of a breach and how quickly. This standard varies by U.S. state while the GDPR has its own timeline.
3. What are the roles for Members in the Data Co-op?
4. What happens if a new party would like to join the Data Co-op and become a party to the Data Co-op Agreement? Should they have immediate rights to this resource, or only when they contribute data?
5. What happens if a Member wants to cease its participation in the Data Co-op and terminate its involvement in the Data Co-op Agreement? Does their data stay in the Data Co-op, or should it be destroyed? What about sponsored studies that rely on their data? Is it "their data" anyway once it has been given to the Data Co-op?
6. Under the GDPR, there is the right to delete, so in that jurisdiction if an individual were to leave the Data Co-op, they could request any personal information be wiped. Determining ownership for data is important because it determines consent for that data to be used in the co-op.
7. What happens to the data and the value to individual members if the Data Co-op is dissolved?
8. What antitrust and anti-competitive issues are relevant to the Data Co-op?
9. What is acceptable usage of the Data Co-op for research, quality, and operational purposes?
10. Is any Personal Identifiable Information (PII) being included in Data Co-op, and if so, what type of information is it?
11. PII is held to strict standards under the GDPR, and depending on the type of data, it could be subject to U.S. federal law. If and how this data is held may be important to ensure compliance with applicable law.
12. Should there be a fee for Member admittance into the Data Co-op?
13. Will agreements exist between Members and third parties that prevent

third parties from being "unjustly enriched" if able to make a novel discovery from the data? How is intellectual property handled in the Data Co-op?

14. What technological standards are required of Members to be eligible to join the Data Co-op? Is a minimum type of Data Co-op Infrastructure required so a Data Co-op can exist in the first place?
15. How do we resolve the technological, economic, regulatory, and social hurdles surrounding the creation of Data Co-ops?
16. How do we establish reliable and secure mechanisms to track the source of data as it is transferred and stored?
17. How do we develop privacy-preserving machine learning methods for pooling data and unlocking insights from that pooled data?
18. How do we establish helpful regulations, consistent across jurisdictions, regarding privacy, data reuse and deletion, data interoperability, and portability?
19. How do we establish standards and processes to fairly value and price individual data contributions within a Data Co-op and how do we establish smooth process to collect and distribute value to the Co-op members?

VIII. ALTERNATIVES TO, AND VARIATIONS OF, THE DATA CO-OP TO PROTECT DATA THROUGH NEW OR MODIFIED CORPORATE STRUCTURES

Below, this Article digs further into vehicles to protect and harness data through an array of existing, modified, and potentially new business structures, as well as through an exploration of imbuing data with the status of corporate-hood and personhood.

There are several paths by which we might establish policies, revise existing law, or create modified viable business structures to better safeguard end user data and to harness the policies, processes, and concepts into some semblance of what I describe herein as a Data Co-op. These solutions require varying degrees of complexity or government involvement (*e.g.*, statutory revisions), but some might be readily deployable without government involvement. I have noted below several of these possible structures and approaches.[181]

181. This article does not explore potential negotiated policy solutions to protect user data from exploitation by online platforms. For instance, perhaps there could be a brokered solution to the Communications Decency Act Section 230 ("CDA 230") dilemma over, in which platforms are largely free to of any liability for hosting defamatory, inflammatory, false, and other potentially harmful content. In order to ensure the protections afforded by CDA 230 protection, the online platform might agree to commit to not exploit or otherwise use data without explicit approval by the user. We have seen similar arguments suggesting that, if a company wants CDA 230 liability protection, the venture should commit to limit, reveal, or allow auditing of its algorithms that were designed to push more and more content to end users in order to maximize online engagement and advertising revenue. *See* CONG. RSCH. SERV., LIABILITY FOR ALGORITHMIC RECOMMENDATIONS (R47753 2023). Or we could implement a takedown process for

If there were to be a function for a government body to provide an opportunity for heightened security and protection of citizen/resident/user data, perhaps a state committed to data protection could simply modify its business organization statutes to allow for the creation of data-sanctifying C-Corps, LLCs, Benefit Corporations, or Co-Ops themselves. States in recent years have passed statutes to promote all sorts of new corporate structures for modern purposes (*e.g.*, promotion of social enterprises through Public Benefit Corporations, Low-profit Limited Liability Corporations, Flex-purpose Corporations; promotion of blockchain-enable corporations like Vermont's BBLLC (blockchain-base LLC) or Wyoming's expansion of its Limited Liability Company Act to allow for blockchain-based ventures and DAOs.) The LLC itself is only about forty years old and was established to provide for more flexibility in corporate structure and governance beyond the traditional C-Corp. None of the state statutorily-created corporate structures have dealt exclusively or even predominantly with the goal of creating privacy-sanctifying corporate structures. A state could modify its own corporate statutes to allow for a straight-forward creation of Data Co-ops with heightened rights and responsibilities to safeguard the data of its members/users. Statutory confirmation that data is to be protected would go a long way to counter the argument that end users have somehow abandoned their privacy interest in their data, once that data is accessible online.

In the BLIP Clinic, my students and I, among other activities, help with startup venture corporate formation. Oftentimes, our clients would like us to create more technologically-robust, procedurally-agile, and socially-responsible corporate structures. More often than not, we run through the hurdles with our clients only to conclude that a traditional C-Corp, S-Corp, or LLC is the most viable business structure for the new entity. This is in large part due to the ease of creation, the business stability, the legal certitude, and the historic and broad acceptance by business, financial, and government players. This, however, need not be the case going forward. Fifty years ago, there was no such thing as an LLC, which is now eminently mainstream. Fifteen years ago, few ventures were willing to go through the aggravations (procedurally and financially) to establish themselves as some form of socially-responsible enterprise, be that a B-Corp[182] certified venture, a Benefit

users to request removal of their data akin to the DMCA 512 takedown process or the GDPR's Right to be Forgotten. *See, e.g.,* 17 U.S.C. §512(c)(3); Regulation (EU) 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), art. 17, 2016 O.J. (L 119).

182. These new-fangled social enterprises with modified processes to advance various public interest objectives demonstrate that there is a great opportunity for socially-minded entrepreneurs and advocates to promote objectives other than shareholder return on equity. The B-Corp, itself, is a model that has not necessarily worked for all public-spirited entrepreneurs. A small startup-working out of a garage or apartment might not even be able to satisfy the rubric required to be a B-Corp or Public Benefit Corporation. The venture might be too small to have employees or physical space and therefore might fail to satisfy enough of the criteria to demonstrate that the venture has virtuous employee or environmental practices. Such micro-ventures are no less virtuous simply because they cannot demonstrate adherence to

Corporation, or any of the experimental socially-responsible corporate structures such as L3Cs[183] or Flex Purpose Corporations.[184]

Imagine a jurisdiction that were to create a simple process for self-organizing and incorporating of legally recognized Data co-ops. Such a jurisdiction would become the test lab for user control and empowerment in a world in which corporations and government are ferociously exploiting user data. The task at hand seems to be to enact a law and establish a straight-forward process for the creation of data co-ops.

A. The Data Co-op itself

Most obviously from the context of this Article and considered extensively *supra*, the state could simply allow explicitly for the creation of Data Co-ops as discussed and described above. Such Data Co-ops could either be distinct corporate entities or modifications of more traditional co-ops. Ideally, the state would work out streamlined processes and incentives to encourage the establishment of Data Co-ops as preferred corporate types.

B. D-Corp: Old Structures Put to New Use: Reimagining the C-Corp Entity as a Means of Creating Data Corp to Protect User Privacy

A state could allow for the creation of a new corporate entity, a modified C-Corporation designed to protect user data (a "Data Corporation" or "D-Corp"). By assigning ownership rights of personal data to individual shareholders in the form of a single share of stock, this model aims to protect privacy rights and provide a more equitable distribution of data control. Below is a legal theory behind the model and its practical application.

The D-Corp model aims to protect user data, including subverting the Third-Party Doctrine by ensuring individuals maintain control over how their information is used, shared, and monetized. By maintaining some form of collectively-owned entity, these individuals could bargain with other entities in the marketplace to release their data in an aggregated, anonymized form, without ever turning over individual data to a "third-party." The rationale behind this model is grounded in property law, which generally provides

---

certain B-Corp criteria, or do not have sufficient funds to pay for an audit. These ventures, however, might have other ways to demonstrate their noble purpose not considered by the B-Corp rubric. Another set of rubric for such micro-ventures could be established. *See The Open Source Definition*, OPEN SOURCE INITIATIVE (Feb. 22, 2023), https://opensource.org/osd/. My students and I in the BLIP Clinic have, over the years, worked on various sets of rubric to allow for alternatives to the B-Corp and Public Benefit Corporation that would prioritize issues that would be most important to bootstrapped social entrepreneurs, such as open sourcing code, releasing copyrightable content through Creative Commons licensing, refusal to prosecute their patents, or even posting their inventions publicly without seeking patent protection so that no one else may try to seek or claim patent protection for the same idea.

183. Sandra Feldman, *What Is an L3C (Low-Profit Limited Liability Company): An Entity for Entrepreneurs Who Value Purpose and Profits*, WOLTERS KLUWER (Mar. 3, 2020), https://www.wolterskluwer.com/en/expert-insights/what-is-l3c-low-profit-limited-liability-company.

184. Linda J. Rosenthal, *Business Fundamentals: Flexible Purpose Corporations*, FOR PURPOSE L. GRP. (June 27, 2013), https://www.fplglaw.com/insights/what-is-a-flexible-purpose-corporation/.

stronger protection for property rights than privacy rights. By demonstrating an individual's clear ownership rights over their personal data, the D-Corp model seeks to create a legally enforceable interest in that data, which could help counteract the effects of the third-party doctrine.

This leaves the question of how best to structure the entity. While there exist various state-authorized legal entities designed specifically for cooperative governance, none have yet become widely adopted and tested by the judiciary, and so each will struggle to attract investment and scale. By contrast, the C-Corp structure has become the gold standard for investors. So long as we can take this existing structure and offer a means of tailoring it to serve as a Data Co-op, we can more easily empower the creation of companies that better protect consumer data without the need to road test a more experimental entity type (or develop an entirely new one).

Described most simply, a D-Corp would assign a single stock to an individual in exchange for the D-Corp's governance of a specific aspect of their data. A second entity, owned by the first but offering a special class of preferred stock to the D-Corp's founders and employees, would manage the collection of the data and negotiate as an agent on the D-Corp's behalf. However, the D-Corp's bylaws would govern the assignment of rights to any information it owns based on the cumulative votes of its users, effectively democratizing control over personal data.

The first step in the formation of a D-Corp (simply a C-Corp with the additional data protection language and processes baked into the bylaws) would be to establish a C-Corp under state law. Like any other C-Corp, this would require the selection of a corporate name, the filing of articles of incorporation, the appointment of a board of directors, and the drafting of corporate bylaws. However, the bylaws of the corporation must be carefully drafted to ensure that they reflect the unique objectives of the D-Corp. Key provisions would include the assignment of ownership rights over personal data to individual shareholders, the establishment of voting mechanisms for decision-making, and the implementation of safeguards to prevent the abuse of data access.

Upon entry into the D-Corp, members would receive a single share of stock in the corporation. This share would represent their ownership interest in the data held by the corporation and entitle them to vote on matters related to the management and use of that data. Users could be asked to vest their stock, ensuring they actually contribute data before being granted voting rights.

To facilitate the collection, storage, and sharing of personal data, a secure and user-friendly platform must be developed. This platform will serve as the primary interface between the Data Co-op and its members, allowing them to provide data in exchange for stock and participate in decision-making processes related to data use. This would also serve as a means of rewarding the founders and employees of the corporation. This should be formed as a subsidiary to the D-Corp, with special preferred stock given to those founders and employees.

As members join the D-Corp, they would provide personal data as consideration for their share of stock. This data would be owned and managed by the corporation in accordance with its bylaws and the decisions made by its shareholders.

The D-Corp model must comply with all applicable laws and regulations, including data protection and privacy laws such as the GDPR in the European CCPA in the United States (so long as such laws would be applicable to the business). Compliance efforts should include the appointment of a data protection officer, the development of data protection policies, and the implementation of appropriate technical and organizational measures to ensure the security and integrity of personal data.

Once the D-Corp is operational, its members would need to engage in ongoing decision-making processes related to the use, sharing, and monetization of personal data. This would involve voting on various matters, such as the establishment of data sharing agreements, the adoption of new privacy-enhancing technologies, and the approval of revenue-generating activities.

In the event of disputes or conflicts of interest among shareholders, the Data Co-op's bylaws should provide clear mechanisms for dispute resolution, such as mediation, arbitration, or litigation. Enforcement of the co-op's rules and decisions may also involve engagement with regulatory authorities or the courts, as necessary.

While the D-Corp model presents a promising approach to protect user data, several challenges and considerations must be addressed for successful implementation:

1. Scalability: As the number of members in the D-Corp grows, decision-making processes may become more complex and difficult to manage. The D-Corp will need to find effective ways to ensure that all shareholders can participate in decision-making without overwhelming the system.
2. Funding: The D-Corp model requires significant investment in infrastructure, legal, and regulatory compliance efforts. The corporation will need to identify sources of funding, such as member contributions, grants, or investment capital, to support its operations.
3. Data Security: Ensuring the security and integrity of personal data is paramount in the D-Corp model. The corporation must invest in robust security measures, including encryption, access controls, and regular audits, to protect against data breaches and unauthorized access.
4. Public Perception and Adoption: Convincing individuals to join the Data Co-op and trust the corporation with their personal data may be challenging, particularly in light of widespread privacy concerns. The corporation will need to develop and maintain a

> strong reputation for transparency, accountability, and ethical data management practices to attract and retain members.

The D-Corp offers a potentially effective means of subverting the third-party doctrine and protecting individual privacy rights. By granting individuals ownership rights over their personal data and democratizing control over data use, the model seeks to empower individuals and mitigate the negative effects of the third-party doctrine. While implementation challenges exist, the D-Corp model provides a promising path forward for those interested in exploring innovative approaches to data privacy and ownership.

Consider a social media company. Users would, before entering the network, agree to enter a collective data ownership agreement, where they would receive one stock in exchange for their participation and contribution of data. The platform itself would be designed and run by a second entity, which, serving as the agent of the first entity, would create and maintain the social network as a mechanism for collecting data. Any decisions as to what to do with that data would be determined by the bylaws of the cooperative company, enacted with the explicit overview and approval of the users. At no point would users ever relinquish control over their data to a third party, only ever deciding to bargain collectively.

C. D-LLC

Rather than establishing the D-Corp as a new corporate structure, with all the corporate formalities of a C-Corp, a state could also permit for the creation of a Data Limited Liability Company ("D-LLC") wherein users would revocably assign their data to the D-LLC. A D-LLC could allow for a lot more flexibility than a D-Corp. A state could simply require a D-LLC to adhere to certain rules, such as state already require for a nonprofit of public benefit corporation. A state could require that, in order to be recognized as a D-LLC, the entity must adhere to certain data use principles such that rather than having a fiduciary duty to maximize shareholder value, the D-LLC would have a fiduciary duty to maximize data contributor protection.

Perhaps the state could encourage the creation of D-LLCs by relieving such entities of some of the archaic, legacy requirements imposed upon traditional LLCs. For example, New York requires all LLCs to satisfy a "Publication Requirement" which could cost up to $1000, a tough hurdle for many bootstrapped individuals and ventures. With online publication free and easy, it seems archaic to compel LLCs to declare their formation in print publications, when online notice would be far cheaper, simpler, and provide more corporate transparency.

D. Guardian ad Datum

While the protections offered to those participating in data co-ops, data trusts, D-Corps, D-LLCs (or other related corporate vehicles that might exist or could be imagined) provide for some protections, there may still be

arguments that none of these entities overcome the perils of the Third-Party Doctrine (although, if done properly, with all data residing with the end-user (*i.e.*, the first party), the Data Co-op may provide protection against warrantless access). By virtue of sharing data with another entity, the participants subject such data to potential compulsory exposure to government agencies. However, new structures of corporate entity or recognition of a particularized legal relationship could help natural persons defeat the Third-Party Doctrine. Since data shared with another "person" becomes subject to such a doctrine, this new type of entity would need to carry with it certain rights and privileges identical to, and an extension of, those rights enjoyed by natural persons. Namely, when a natural person shares their personal data with this entity, such a transfer of data must not be considered the same as sharing this data with an additional entity. A state could allow for an entity to serve as a *Guardian ad datum* ("GAD"), which would exercise the same rights over the data and its use that a *guardian ad litem* might in a trial, or some sort of *power of data* ("POD") that would allow an entity to act similarly to one who holds *power of attorney* over another.

Such a data-based structure could allow for natural persons to share their data with such an entity that would essentially be legally indistinguishable from the data subject for legal purposes. Custom and usage in the common law world allows for the sanctity of certain relationships between parties where communications and other information shared between such parties is privileged, protected, and subject to compulsory disclosure in the rarest of circumstances. As discussed throughout this Article, the ubiquity of technology in contemporary society creates data trails evidencing our comings and goings over which the user/data creator has little control. By allowing qualified persons, such as lawyers, to serve as the GAD, people can rest assured that a gilded professional, answerable not just to the user, but a board of professional responsibility administered by a state Bar Association, would sit as a guardian over personal data and be required, at the threat of professional sanction and loss of livelihood, to ensure that the data is protected and used only in proper, authorized ways.

E. Data Personhood[185]

Rather than creating (or modifying) a corporate structure in which data protection is paramount, another path worth exploring is the concept of "Digital Personhood", or, perhaps more precisely in this context, "Data

185. There may be other paths beyond new-fangled corporate structures a state might take to better protect user data. One vehicle toward more sovereign data protection could be the expansion of a state's "right to publicity" law to include personal data and metadata which would preclude anybody from appropriating that data for commercial gain without the express grant of a license by the data subject. The right to publicity is simply the right to control commercial use of one's name, image, likeness, and other identifying aspects of identity. It would be a simple matter for a state to recognize the increasing importance of user data as akin to other aspects of one's identity, and to prohibit the appropriation of user data by third parties without explicit consent from the first party.

Personhood." If persons can be persons, if persons can be corporations, if corporations can be persons, if data can be corporations, could data be persons, at least as a legal fiction?

Concepts of Digital Personhood are still typically relegated to the realm of science fiction and rarely given serious consideration in legal processes. Too often law is backward looking and fails to anticipate how technology will disrupt society and legal process. What is becoming increasingly clear is that artificial intelligence, quantum computing, and advances in data science will profoundly affect society in ways for which government, law, and society are not yet ready. This concept is worthy of multiple articles, books, legal opinions, and public debate. This Article only tees up the issue.

Most online, democratically-organized systems rely on one of two methods of decision-making: (1) one economic unit equals one vote or (2) one person equals one vote. Perhaps it is time we were to consider revising this governance model to value data over money or corporeal existence, at least in virtual spaces where data is paramount. We could allow one datum to equal one vote. And, perhaps, these data, as the virtual world evolves, would take on the characteristics and the rights and responsibility that come with personhood. This would not be the same as giving personhood to artificially intelligent beings, because the data would be a virtual embodiment, representation, or significant aspects of a bona fide, recognized, conscious human being.

As digital technology and our ability to create algorithms to quantify and synthesize the universe of data evolve and become more integrated and ubiquitous, everyone and everything could be identified as its own universe of data points. Each "person" may become, at least for digital, online, and virtual purposes, a universe of data points, perhaps a unified, synthesized aggregation of their biometric data, their genome map, other physical and virtual attributes, their particular social graph, and other identifiers of individual identity. This conglomeration of data becomes a digital manifestation of the person. Perhaps it is time to allow this data bundle that replicates the person to have virtual rights equal to the physical rights of a physical human. And, to the same extent that a person's limb or blood or organ arguably cannot be taken without proper legal or contractual process, a person's datum(a) cannot be taken or used without proper legal or contractual process.

We could consider the concept of data personhood as a vehicle to extend privacy protections and other "human" rights to data. As noted by Jannice Käll, Associate Professor of Sociology at Lund University in Sweden, "legal personhood has been extended past the sphere of persons commonly held to such standard in the West."[186] Corporations have evolving status as legal persons. We now could consider an evaluation of "new" human rights in the

186. Jannice K. . .ll, *A Posthuman Data Subject? The Right to Be Forgotten and Beyond*, 18 GERMAN L. J. 1145 (2017). *See also*, JOSHUA C. GELLERS, RIGHTS FOR ROBOTS, ARTIFICIAL INTELLIGENCE, ANIMAL AND ENVIRONMENTAL LAW (Routledge ed. 2021).

digital age, starting first by considering who or what constitutes a person, perhaps taking inspiration from posthumanism.

i. "Corporations are People"

Mitt Romney infamously said, "Corporations are people, my friend."[187] Perhaps this was a contextually tone-deaf comment when he uttered this to an assembly of *human* voters. Such a comment would have required a few paragraphs of legal reasoning to unpack the broad assertion, but from a legal fiction perspective, Romney was largely accurate. There are both statutory and judicial reasons for this reality. From a statutory perspective, the expansion of corporations from single-purpose entities into multi-purpose immortal behemoths with incredibly broad purposes led to the expansion of the sheer number and power of corporations.[188] Today, general incorporation statutes mean that anyone "can file a few administrative papers, pay a few fees, and be the proud owner of their very own corporation."[189] This has resulted in more than two million corporations incorporated annually in the U.S. Corporations may be incorporated for "any lawful purpose," rather than the limited purpose of yesteryear. The Supreme Court has expanded corporations' constitutional rights based on a theory that corporations were "persons" most notably protected by the Fourteenth Amendment, the Fourth Amendment, the First Amendment, and the Contracts Clause.[190] In fact, corporate rights decisions such as *Citizens United* have often been interpreted as victories for the idea that corporations are rights-bearing people.[191] Of particular relevance, Justice Oliver Wendell Holmes noted that "the rights of a corporation against unlawful search and seizure are to be protected even if the same result might have been achieved in a lawful way."[192] Should one's data be treated with any less deference and respect than a corporation?

ii. Data are People?

So, could personhood apply to data? Could we create a concept of Data Personhood with vested rights inuring to the data itself? Personal Data is arguably a more direct manifestation of a person than a "Corporation" and, perhaps, should be afforded a broader set of rights and liberties than

187. Ashley Parker, *'Corporations Are People,' Romney Tells Iowa Hecklers Angry Over His Tax Policy,* N.Y. TIMES (Aug. 11, 2011), https://www.nytimes.com/2011/08/12/us/politics/12romney.html.

188. Louis K. Liggett Co. v. Lee, 288 U.S. 517, 541–586 (1933), 554–56 (Brandeis, J., dissenting). *See* Ciara Torres-Spelliscy, *Does "We the People" Include Corporations?*, 43 ABA HUM. RTS. MAG. (Jan. 1, 2018), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/we-the-people/we-the-people-corporations/

189. *Supra* note 185.

190. *See generally* Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010).

191. Nikolas Bowie, *Corporate Personhood v. Corporate Statehood* 132 HARV. L. REV. 2009 (2019); Adam Winkler, *We the Corporations: How American Businesses Won Their Civil Rights.* xxiv, 471(W.W. Norton & Co. 2018).

192. Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920).

corporations. In the digital world, a person is arguably nothing more than their aggregated data set that defines all the parameters of the person.

Almost 30 years ago, Nicholas Negroponte asserted that, in the past, things made of atoms are all important, and in the future everything that matters would be "made of bits."[193] Negroponte presciently noted that "We are clueless about the ownership of bits. Copyright law will disintegrate ... Bits are bits indeed. But what they cost, who owns them, and how we interact with them are all up for grabs."[194]

Growing out of Negroponte's seminal observations, several scholars have begun to explore the nature of virtual or digital personhood and the embodiment of a human as, itself, a data collective. I shall consider several of these scholarly observations below.

In *Privacy and the New Virtualism*, Jonathon Penney notes that "[p]rivacy scholars have already come to identify bits of information and data (particularly those that reveal intimate details about us) that can be collected by tracking a person's movements on the Internet as constituting a form of virtualized person, or persona."[195] Penney cites Daniel Solove who argues that, "[d]igital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. It is ever more possible to create an electronic collage that covers much of a person's life — life captured in records, a digital person composed in the collective computer networks of the world."[196] Solove refers to the collection of intimate information about a person as a "digital person" or "digital dossier" because of its ability to "offer a detailed and complete mapping of the person."[197] Further, Penney cites Patricia Mell who notes that this electronic "compilation of bits of personal information concerning the individual" can perform a number of different functions for varying parties in the digital context, including acting as an invaluable information resource for governmental and commercial entities.[198]

The concept of data personhood makes more and more sense as we head further down the path into the digital age and the ubiquity of our virtual experiences, lives, and existence. The concept of a virtual person as embodied data aligns with traditional personhood theories of personhood as consciousness and memory.[199] A virtualist point of view requires relinquishing the idea of physical bodies for virtual ones. For example, computerized

193. NICHOLAS NEGROPONTE, BEING DIGITAL (Vintage Books ed., 1995).

194. *More from Nicholas Negroponte*, ELON UNIV., https://www.elon.edu/u/imagining/time-capsule/early-90s/nicholas-negroponte/ (last visited Jan. 22, 2024).

195. Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J.L. & TECH. 194 (2008).

196. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1 (2004).

197. *Id.* at 1–2; *See also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 516–17 (2006).

198. Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 4 (1996).

199. Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J.L. & TECH. 194, 216–17 (2008).

medical health info and electronic databases containing maps of a person's genetic code, biometric info, etc. serve as an individualized "link" between the record and the person.

Nadia Banteka in *Artificially Intelligent Persons*, compares corporate personhood to data personhood, as two artificial entities based on three "theories" of personhood.[200] First, Banteka considers "fiction theory," noting that an "artificial entity is not a person but the law approaches it as if it were to allow these entities to act within the confines of this legal fiction"[201] Second, Banteka considers "symbolist" or "aggregate" theory, noting that "[t]he law gives artificial entities legal personhood as a shorthand for representing and conceptualizing the relations between the natural persons (who are members of the artificial entity) and the entity itself, as well as relations between the entity and the world." (*i.e.*, a "legal person" is equivalent to the sum of natural persons that are its members).[202] Third, Banteka considers "realist theory," noting that artificial entities are objective, exist beyond the law, but the law takes account of them and personalizes them, based on the premise that "artificial entities that are independent, autonomous and act with real effects in the legal realm such as owning property or performing transactions have long existed."[203] Artificial entities exist prior to the law granting them personhood, and continue to exist as legal persons after legal personhood has been granted.[204]

Katherine Hayles in *How We Became Posthuman* focuses on the point at which human bodies are dematerialized as a means to materialize digital elements as independent matter through cybernetic discourse that is "free from the material constraints that govern the mortal world."[205] In turn, dematerialization can be understood as a concept for describing how the human body, as well as knowledge or information, undergoes shifts in materiality through specific narratives for objectifying information. Further, as Käll notes, the blurring of boundaries between humanity and technology "implies that both the body and mind are understood as coded programs of information."[206]

In *Data as Collectively Generated Patterns: Making Sense of Data Ownership*, Mathias Risse, Faculty Director of the Carr Center for Human Rights Policy and Berthold Beitz Professor of Human Rights, Global Affairs and Philosophy, notes that theorists have different approaches to the conceptions of "data as" certain things (*e.g.*, data as oil, labor, salvage, IP, and

200. Nadia Banteka, *Artificially Intelligent Persons*, 58 HOUS. L. REV. 537, 553–55 (2021).

201. *Id.* at 554 (citing Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)). ("[T]he corporate personality is a fiction, although a fiction intended to be acted upon as though it were a fact.").

202. *Id.* at 555.

203. *Id.*

204. *Id.* at 555–56.

205. N. KATHERINE HAYLES, HOW WE BECAME POSTHUMAN: VIRTUAL BODIES IN CYBERNETICS, LITERATURE, AND INFORMATICS 13 (Univ. Chi. Press ed., 1999).

206. K. . .ll, *supra* note 183, at 1156.

even personhood).[207] By virtue of having been produced by humans, data express aspects of personhood, one way or another.

This approach to data personhood underscores the underlying premise of the Article that humans have as much right to control of their data, their virtualized manifestations, as they would any other essential appendage or thought. Perhaps *Carpenter* is informative here. In *Carpenter*, the Supreme Court made a point to distinguish information gathered from a cell phone from information gathered from a vehicle, to determine whether the Fourth Amendment had been violated, noting that a cell phone is like an appendage of a human body that individuals "compulsively carry" on them at all times.[208] As Lawrence Lessig notes in his seminal *Code 2.0*:

> At least some kinds of information about individuals should be treated differently .... Individuals should be able to control information about themselves. We should be eager to help them protect that information by giving them the structures and the rights to do so. We value, or want, our peace. And thus, a regime that allows us such peace by giving us control over private information is a regime consonant with public values. It is a regime that public authorities should support.[209]

IX. CONCLUSION

Cycles of technological development since the industrial revolution adhere to a predictable pattern of diffusive democratization followed by a technocratic contraction that recentralizes control in a small number of powerful players that fall subject to government regulation and coercion. Many recent technology providers have followed the ad-supported model of connected services first adopted by tech giants like Google, Facebook, and X (formerly Twitter). These companies collect and exploit users' personal and behavioral for tremendous profit and share such data with government agencies out of a combination of fear of regulation and the so-called Third-Party Doctrine, which exterminates Fourth Amendment protections for data shared with third parties. Using existing legal structures such as trusts or co-ops, groups of individuals may band together to exercise greater control over their personal data. Once a user has regained control over their personal data through a Data Co-op, Data Trust, or similar fiduciary-based vehicle, such user may make decisions about how that data about them is shared, use, and/or monetized, and potentially combat expansive Third-Party Doctrine-based demands from government agencies.

However, while trusts and co-ops have existed for decades, Data Trusts and Data Co-ops are still new, novel structures. Absent a significant corpus of

---

207. MATHIAS RISSE, DATA AS COLLECTIVELY GENERATED PATTERNS: MAKING SENSE OF DATA OWNERSHIP 1 (Carr Ctr. Hum. Rts. Pol'y. Harv. Kennedy Sch. ed., Spring 2021), https://carrcenter.hks.harvard.edu/files/cchr/files/210426-data_ownership.pdf.

208. Carpenter v. U.S., 138 S. Ct. at 2217.

209. LAWRENCE LESSIG, CODE: VERSION 2.0 231 (Basic Books ed., 2006).

court decisions addressing issues around these structures, lawyers and consumers are left to speculate as the extent these structures will be recognized by private and public interests with respect to protection of personal data from expansive government intrusion. Perhaps the creation and/or recognition of a new structure and fiduciary relationship, such as the *Guardian ad Datum*, could solve for this conundrum and allow individuals to share with an entity their personal data to ensure such data is put to good use and remains safe from government overreach. Or, ultimately, perhaps recognition of data corporate-hood or data personhood, with virtual rights inuring to the data itself, could prove to be an answer to valuing our data as we value ourselves.