PERSONAL DATA EASEMENTS

SARAH LAMDAN*

This article explores the concept of personal data easements to balance data ownership rights with the privacy rights of data creators. Conceptualizing personal data as property is not new; the idea was widely discussed in the early 2000s when it became clear that there would be a personal data industry, but the idea was effectively tossed aside in favor of allowing data companies to regulate themselves. Self-regulation has resulted in a digital ownership scheme that lacks balance. All of us create data exhaust (private data about ourselves), but we do not own it. Instead, that exhaust is collected and monetized by private companies, often without our knowledge and consent. In essence, companies treat our personal data like their property.

Individuals' data is a unique informational product because it is simultaneously very personal to its creator and very profitable for the third parties who claim ownership of it. It's separate from digital infrastructure, including databases, and more intimate, but it's also different than traditional intellectual property, real property, or other tangible property. It is factual material, not an original creation of the mind. It is also invisible, free-flowing, and seemingly ethereal, lacking the characteristics of tangible property.

Legal scholars have explored property law solutions to balance ownership and access interests in digital infrastructure including databases, platforms, and internet service providers. This article considers property law solutions for the personal data that fuels that infrastructure, populating many of today's databases and fueling data analytics and artificial intelligence products. It focuses on easements as a model to balance the interests of companies that use and exploit personal data against the interests of people who want to regain control of their digital exhaust.

Because the easements model is not an all-or-nothing ownership model, it allows for positive digital innovations while preserving people's privacy rights.

INTRODUCTION

Personal data has become a critical resource, powering policing systems, social media platforms, and the apps we use for everything from buying bread to finding a mate. Despite its prevalence, the question of who has the right to own and control personal data remains unsettled.[1] In the status quo, the entities that own our personal data also control the data rights and access in full.[2] Legislators and legal scholars have suggested that we impose an opposite scheme where every individual controls their own data dossiers.[3] Neither of these approaches work; they are both ownership extremes.[4] Leaving the market in charge of personal data leaves individuals with no rights in their data, but giving everyone full ownership rights to their data could slow technology and communication to a crawl as companies scramble to obtain people's data rights one by one.[5] What if instead, ownership could

* Professor of Law, CUNY School of Law. Professor Lamdan would like to thank Belmont Law Review's editors and symposium organizers for facilitating discussions around this work and for improving the article throughout the revision process. She would also like to thank her research assistant, Harshini Gorijala, for providing research and insights about data privacy and property law.

1. *See generally* SARAH LAMDAN, DATA CARTELS: THE COMPANIES THAT CONTROL AND MONOPOLIZE OUR INFORMATION 47–48 (2022).

2. Meg Leta Jones, *Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw*, 2018 U. ILL. J.L. TECH. & POL'Y 249, 253 (2018).

3. *See* Own Your Own Data Act, S. 806, 116th Cong. (2019) ("Each individual owns and has an exclusive property right in the data that an individual generates on the internet"); Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 348 (2021) ("Given the increasing value of data to consumer choice and market efficiency, we are inclined to adopt a more expansive definition of consumer data in order to ensure that consumers have control over their information").

4. LAMDAN, *supra* note 1, at 47–48.

5. *Id.*

be split, giving some rights to personal data back to the data creators? Is there a model for this type of arrangement in property law doctrine that is already used to govern ownership in the physical world?

When the current personal data market first emerged in the early 2000s,[6] the idea of applying property rights to personal data was raised, investigated, and dismissed as unworkable.[7] These past iterations of personal-data-as-property were envisioned in a different digital era, one wherein there were no online platforms and no cloud computing systems; before the personal data industry was so pervasive.[8] In the early 2000's, people formulated plans for the ownership of personal data based on pre-existing physical ownership models. Legal scholars and policymakers imagined people setting up personal information accounts similar to bank accounts in a "National Information Exchange."[9] They envisioned each of us depositing and withdrawing our data as we chose.[10] The idea of information banks presented a creative solution for balancing personal data ownership by making the exchange of data into a market transaction, but even its creators saw the economic, social, and legal problems inherent in a personal data exchange and knew that it would require a "revolution in American property law."[11]

The idea of applying property law to technology was also a political dud in the early 2000's.[12] A lack of urgency and a fondness for laissez faire market governance makes regulating personal data, or passing laws that could stifle technological growth, unappetizing. The legislative process tends to be a post hoc affair, spurred by disaster.[13] Environmental law emerged only after rivers caught fire and deadly smog suffocated towns.[14] The most powerful securities laws are legislative reactions to market crashes.[15] In 2000, one could imagine personal data disasters, but few, if any, had actually transpired.[16] It's no surprise that 2000-era scholars said treating personal data

---

6. This investigation of rights was prompted by the rise of platforms like Facebook and Amazon, which depended on personal data to connect and sort us.

7. As legal scholar Mark Lemley put it, succinctly, "'there is no good market solution' for information privacy based around property rights." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2077 (2004) (quoting Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1554 (2000)).

8. *See id.* at 2076–77.

9. Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1136 (2000) (citing Kenneth C. Laudon, *Markets and Privacy*, Commc'ns. ACM, Sept. 1996 (Loudon's description of an actual infrastructure for data ownership)).

10. *See id.*

11. Kenneth C. Laudon, Markets and Privacy, Commc'ns ACM, Sept. 1996., at 99–101.

12. LAMDAN, *supra* note 1, at 21.

13. *Id.* at 24.

14. *Id.*

15. *See generally id.*

16. *Id.* at 23–24.

like personal property was "bad politics."[17] They knew that, until there was some sort of catalyzing event, the government would allow tech companies and data owners to protect their rights to do what they want with our data.[18]

Now in 2022, however, it's easier to point to data privacy problems.[19] In recent years, the over-the-top use of our personal data in creepier ways, including in predictive policing products, ad-targeting, election-deciding, and most recently, abortion-tracking, has made politicians more interested in data privacy.[20] These uses are eroding some of the shine from personal data products, and the public is growing more critical of personal-data-powered products. Political headwinds are changing in response to these creepy personal data enterprises, and people are starting to push for government intervention to limit the data brokering industry. Since the data landscape has changed, we should take advantage of the favorable political headwinds and revisit solutions that analogize personal data as property to other types of property.

Although putting personal data problems into a property law framework has been dismissed, in the past, as practically complicated and politically fraught, property law solutions are not, in themselves, bad ideas.[21] Digital property ownership is often envisioned as absolute; either corporate or governmental data owners own people's data in full, or individual people do.[22] In reality, however, property law is rarely absolute.[23] Even though there are owners and non-owners, property law provides exceptions and points of access to balance interests between property stakeholders.[24] Property law was meant to balance the interests of property owners with the public interest, not to confer absolute, indivisible ownership in one party in every case.[25] Lawmakers devised ways to respect both private ownership and public access needs because they recognized that owning resources like land and water was crucial to development, commerce, and innovation.[26] But they also realized that, in some cases, those critically important resources should not be

17. *See* Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1547 (2000).

18. *See id.* at 1547.

19. *See generally* LAMDAN, *supra* note 1, at 1–2; *see also* Kolawole Samuel Adebayo, *Why privacy and security are the biggest hurdles facing metaverse adoption*, VENTUREBEAT (Nov. 10, 2022), https://venturebeat.com/virtual/why-privacy-and-security-are-the-biggest-hurdles-facing-metaverse-adoption/ [https://perma.cc/SUL9-RCEM].

20. *See* Rebecca Lipman, Online Privacy and the Invisible Market for Our Data, 120 PENN ST. L. REV. 777, 780–81 (ad-targeting); *see also* LAMDAN, *supra* note 1, at 27.

21. *See generally* Samuelson, *supra* note 9, at 1130–36 (discussing the appeal of a property rights approach).

22. *See* Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 OR. L. REV. 695, 737 (2003).

23. *Id.* at 730–31.

24. LAMDAN, *supra* note 1, at 128.

25. *Id.*

26. *See generally* Schwartz, *supra* note 7, at 2084–85.

exclusive—there are situations where people besides owners should have access to and rights to water, land, and other real property.[27]

The concept of personal data as property is complicated, in part, because, personal data is hard to compartmentalize in the existing property law scheme. Intellectual property law is commonly applied to creative digital content including digital code and built digital infrastructure, property law principles are not ordinarily applied to factual personal data.[28] This is not surprising as personal data is, practically, very different than other types of informational property.[29] As information, personal data lies somewhere between creative intellectual property and facts. It isn't a "product of the mind," but it is connected to us in a way that other facts, such as stock prices and sports statistics, are not.[30]

In addition to its unique informational qualities, personal data is also unique as a marketplace good.[31] Personal data has become a commodity, similar to oil, charcoal, or timber, which are treated like physical property according to the law.[32] Oil and charcoal fuel our physical industries, and personal data is the fuel that powers many modern technological innovations. Weather apps, digital maps, and social media platforms would be hollow algorithmic shells without personal data.[33]

Personal data is tough to regulate because it has a unique form and unique functions that put it on the property law spectrum somewhere between intellectual and physical property.[34] It is both an essential, critical resource for technological industries and an intangible collection of intimate, personal details.[35] Some scholars have suggested using public easements on social media platforms to protect speech about issues of public concern.[36] This article argues that, conversely, there should be private easement rights to protect private information. Because ownership determines whether personal data is used for public benefit or public harm, property law—the law of ownership rights—provides a helpful framework for envisioning a more equitable balance between the rights of data-based enterprises and the rights of individual users. Section I explains the current landscape of personal data

27. *See* LAMDAN, *supra* note 1, at 128.

28. *See generally* 17 U.S.C. § 102.

29. *See generally* Lemley, *supra* note 17, at 1548–50.

30. *See* Samuelson, *supra* note 9, at 1140.

31. LAMDAN, *supra* note 1, at 137 ("Each piece of information is unique, while those other resources are fungible and interchangeable.").

32. *See* Eric Buchanan, *Alaska's Explicit Right to Privacy Warrants Greater Protection of Alaskan's Personal Data*, 37 ALASKA L. REV. 25, 26 (2025) ("Personal data has become a lucrative commodity, generating billions of dollars for the private companies that collect it.").

33. LAMDAN, *supra* note 1, at 48.

34. *Id.* at 137.

35. *See generally id.*

36. Ronald J. Krotoszynski, Jr., The First Amendment as a Source of Positive Rights: The Warren Court and First Amendment Easements to Private Property, in The Disappearing First Amendment (2019).

ownership sans any property interest balancing mechanisms. Section II introduces property law as a framework for balancing data companies' interests in personal data with the interests of data subjects. Section III focuses on easements as a particularly helpful analogy that could be enacted in personal data legislation. A personal data easement model would ensure that people have access to, and some control over, their data dossiers, while still allowing useful, public interest-focused data innovation to flourish.

I. PROPERTY LAW IS A USEFUL FRAMEWORK FOR DATA PRIVACY, NOT A SOLUTION

This article focuses on property law as a solution for modern data privacy problems, but property law is not a silver bullet that will ameliorate people's personal data concerns. Data privacy is a multi-faceted issue that involves an array of overlapping legal issues. Many entities use personal data. Some of these entities are state actors subject to constitutional and administrative law requirements about warrants and data privacy.[37] Others data users are not subject to those obligations. Personal data is also so varied, and used for many varied purposes that deserve different legal treatment. For instance, Congress treats children's data differently than adults' data, and it has treated our healthcare data, educational data, and financial data as deserving of special protections.[38] Finally, property law doesn't deal with perhaps the biggest problem: big tech monopolies. In order to truly empower consumers, antitrust law enforcement must ensure that consumers can opt out of data collections and that there is sufficient competition in tech sectors so that consumers can choose products that do not commodify their personal data.

Another reason that property law doesn't provide easy solutions to data privacy is because common and statutory property law concepts predate the complexity of our current personal data schemes. The lawmakers who drafted the laws and policies we currently apply to personal data wrote their rules decades ago, before we had iPhones, social media, and predictive policing products. Most of our current privacy and data protection laws were enacted before the internet even existed. They are "ill-equipped to regulate today's informational infrastructure."[39]

Ultimately, we will need new laws (or major reformations of existing laws) to create an equitable personal data system that both allows for tech innovations and allows people to participate equitably choices about how their personal data is collected and used. Our existing legal frameworks will

37. *See, e.g.*, U.S. CONST. amend. IV; Privacy Act of 1974, 5 U.S.C. § 552a.

38. *See, e.g.*, Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501–6505; HIPAA Privacy Rule, 45 C.F.R. §§ 164.500–164.534 (2021); Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681.

39. Lamdan, *supra* note 1, at 21.

not solve today's personal data policy problems. That doesn't mean that lawmakers must ignore the centuries of legal knowledge captured by our current legal schemes. Property law and other traditional legal doctrines may not be the best for regulating data problems, but policymakers *can* borrow concepts from the past to address the data problems of today. As information law scholar Jacqueline Lipton suggests, even if policymakers don't directly adopt property law principles in a data context, the concepts provide a "useful shorthand" guide for addressing digital information issues—so long as they are used appropriately.[40] This type of cognizable shorthand helps law and policymakers make sense of the digital world using a familiar legal language.[41] Imbuing personal data with property law-styled balances would provide more personal data protections than the current data industry provides, with solutions that lawmakers, courts, and legal practitioners are familiar with.[42]

A. How the Personal Data Industry Operates Without Property Interest Balancing

In the thirty years since Hank Asher, the "father of data fusion," developed his first personal data product for the police, people's data has become a major digital good.[43] Today, personal data is a material that companies buy, sell, and barter like other property.[44] Personal data, including our DNA and health outcomes, is treated more like other portfolios of extracted assets (timber, oil, etc.) and less like an intimate byproduct of human life.

When people do their shopping, dating, research, and healthcare online, they leave digital markers of their activities. Every click is collected. Just as automobiles emit clouds of exhaust as they travel on roads, humans emit data exhaust as they travel around the internet, leaving clouds of datapoints in their wake.[45] These datapoints are owned by third parties, not

40. Lipton, *supra* note 22, at 710.

41. *Id.* at 711.

42. *See id.*

43. Michael Shnayerson, *The Net's Master Data Miner*, Vanity Fair (Dec. 1, 2004), https://www.vanityfair.com/news/2004/12/matrix200412 [https://perma.cc/YBW2-Y3W2].

44. *See* Leonard Murphy, *Personal Data: The Ultimate Commodity?*, GREENBOOK: BLOG (Sept. 21, 2017, 6:09 AM), https://www.greenbook.org/mr/market-research-news/personal-data-the-ultimate-commodity/ [https://perma.cc/ABK2-MZ85].

45. Compare McKay Cunningham, *Exposed*, 2019 MICH. ST. L. REV. 375, 379 (2019), *with Greenhouse Gas Emissions from a Typical Passenger Vehicle*, U.S. ENV'T PROT. AGENCY (last updated June 30, 2022), https://www.epa.gov/greenvehicles/greenhouse-gas-emissions-typical-passenger-vehicle [https://perma.cc/MJD3-Z4DX]; *see also* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Know*, FORBES (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=ad12a4460ba9 [https://perma.cc/2SRB-UWLJ].

the people who emit them, and those third parties buy and sell them.[46] As the "internet of things" expands, every product is becoming a data-collecting product.[47] Home appliances including refrigerators, thermostats, and even the machines that make people's morning coffee gather information about consumer choices.[48] In addition, thermometers, watches, and medical devices placed inside human bodies by doctors are also data siphons.[49] Even if someone lives in an appliance-free cave and wears a flour sack, their data will still be collected by cameras, drones, and other devices embedded into public spaces.[50] In short, if an individual exists in society, some third party owns a dossier of their personal data.[51]

Because of all of the new ways to collect and use personal data, the personal data industry is booming.[52] Largely unfettered by government intervention, data brokering and data analytics companies, collectively, make billions of dollars by selling and using people's data exhaust.[53] One reason they can rake in profits is that personal data is usually free—people trade their data in exchange for access to digital platforms, products, and services.[54] Unlike intellectual property, personal data's creators don't consensually or, in many cases, even consciously hand over ownership rights to their data.[55]

---

46. *Your Data Is Shared and Sold…What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/WCA6-RJSE].

47. Jen Clark, *What is the Internet of Things (IoT)?*, IBM BUS. OPERATIONS BLOG (Nov. 17, 2016), https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ [https://perma.cc/325N-Y6Z6].

48. Anick Jesdanun, *Home Items Are Getting Smarter and Creepier, Like It or Not*, AP NEWS (Jan. 7, 2019), https://apnews.com/article/nv-state-wire-north-america-technology-lifestyle-business-12787de930564f2cbe8fadfdf63e2e7e [https://perma.cc/R6HU-WUXH] (refrigerators and thermostats); Nina Trentmann, *Keurig Dr Pepper's Data Tracking Helps in Making Financial Forecasts*, WALL ST. J. (Aug. 6, 2020, 6:36 PM), https://www.wsj.com/articles/keurig-dr-peppers-data-tracking-helps-in-making-financial-forecasts-11596753392 [https://perma.cc/4FDU-8CYM] (coffee machines).

49. *See* Angela Foster, *Legal Implications of Data from Wearable Devices*, 42 LITIG. NEWS 26, 26–27 (2016).

50. *See generally* Rebecca L. Scharf, *Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy*, 94 IND. L.J. 1065, 1096–100 (2019) (discussing how drones will collect personal data and the policies underlying these issues).

51. *See* David R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 589 (2014) ("Dossiers of where we go and with whom we meet are created automati[]cally as we go through our daily lives. They reside with cell phone, Internet, search, email, e-commerce, credit, and almost any service we use.").

52. *See* Jathan Sadowski, *When Data is Capital: Datafication, Accumulation, and Extraction*, 6 BIG DATA & SOC'Y 1, 2 (2019) (observing the rapid growth of the digital economy).

53. *Id.* at 8.

54. Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data [https://perma.cc/WHE5-96RY].

55. *See id.*

The data industry often gets lumped in, or conflated with, the systems and industries that use it, but data is separate from digital infrastructure, including the databases, platforms, and apps that it feeds. Data is the fuel of the internet and digital applications. It is a raw material used to create informational products.[56] Apps require our geolocation data to work.[57] Biometric data is a necessary resource for health apps that track insulin levels,[58] predict fertility,[59] and ensure the user's heart rate stays within healthy bounds during exercise.[60] Social media companies, predictive data analytics ventures, and databases all rely on data as a core ingredient of their informational products, but personal data is independent from those systems.[61]

Users cede their data to third-party companies because these data-digesting apps and platforms improve daily life.[62] Using digital filing forms and services for banking, shopping, and other errands has saved people countless hours and trips.[63] During the COVID pandemic, digital services protected their users from potentially deadly infection.[64] Personal data-driven technology is miraculous. It connects people continents away and expands what is possible in the world. Without personal data and information, weather and map apps wouldn't be able to seamlessly provide forecasts and directions. Facebook and TikTok would not be able to generate their

56. *Cf.* Julie E. Cohen, *The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213, 213 (2018).

57. *See* Anzhela Sychyk, *What Apps Make the Best Use of Geolocation Services?*, DATADRIVENINV. (Jan. 27, 2020), https://www.datadriveninvestor.com/2020/01/27/what-apps-make-the-best-use-of-geolocation-services/ [https://perma.cc/8W6D-GHT5] (discussing apps that rely on geolocation services).

58. Kacie Doyle-Delgado & James J. Chamberlain, *Use of Diabetes-Related Applications and Digital Health Tools by People with Diabetes and Their Health Care Providers*, 38 CLINICAL DIABETES 449, 449 (2020).

59. Maryam Mehrnezhad, *Fertility Apps and Cybersecurity: Who Can Access Your Data?*, NEWCASTLE UNIV., https://from.ncl.ac.uk/research-fertility-apps-and-cybersecurity [https://perma.cc/2EYW-G4PE] (last visited Nov. 5, 2022).

60. *See, e.g.*, *Monitor Your Heart Rate with Apple Watch*, APPLE (Sept. 12, 2022), https://support.apple.com/en-us/HT204666 [https://perma.cc/PFH5-FBL6] (discussing how users can activate notifications to monitor their heart rates for exercise and non-exercise purposes).

61. *See* Jon Hill, *Data vs Information: What's the Difference?*, BLOOMFIRE (June 15, 2021), https://bloomfire.com/blog/data-vs-information/ [https://perma.cc/EE4K-TU7B].

62. *See* Anindya Ghose, *Do Health Apps Really Make Us Healthier?*, HARV. BUS. REV. (May 7, 2021), https://hbr.org/2021/05/do-health-apps-really-make-us-healthier [https://perma.cc/NAE3-KG5U] (discussing benefits users gain by utilizing "mHealth" apps).

63. For an example of how baking apps have saved consumers trips to the bank, see Mitch Strohm, *5 Benefits of Digital Banking*, FORBES ADVISOR (Dec. 15, 2021, 4:19 PM), https://www.forbes.com/advisor/banking/benefits-of-digital-banking/ [https://perma.cc/6JJJ-M6R6].

64. Wick Eisenberg, *Predicting a Covid-19 Outbreak? There's an App for That.*, JOHNS HOPKINS UNIV.: HUB (Mar. 24, 2021), https://hub.jhu.edu/2021/03/24/covid-19-app-predicts-outbreaks-based-on-symptoms/ [https://perma.cc/X8FF-DHB5].

addictive informational feeds, and our health apps would not be able to provide timely and useful notifications to their users.

But the same data that powers the greatest modern innovations can also be used in ways that violate privacy and threaten civil rights and liberties. Even though datapoints, like home addresses or blood pressure recordings, on their own, may not seem very useful or personal, in aggregate, a person's personal data creates "an ever-evolving, 360-degree view" of people's lives.[65] The same personal-data-using technologies that have made life more convenient and connected can also be deployed against its data subjects. Personal data products track, sort, and make predictions about people.[66] Some do this on purpose (predictive policing platforms, geospatial tracking), and some do this as an incidental step in their end products or to cultivate a side-business or secondary benefit. (For instance, a food delivery app may provide convenient food service, but it may also have an auxiliary business selling data to restaurant marketing firms.[67]) Data systems can also be intentionally deployed to influence decisions that negatively impact consumers' lives. Personal-data-powered software does everything from ad-targeting to helping institutions make hiring, lending, and insurance decisions.[68] The government uses data companies' products to decide who presents criminal risks, who might commit fraud, and who should be given public benefits.[69] Without transparency or access, individuals have little control over how their data is used.

---

65. McKenzie Funk, *How Ice Picks Its Targets in the Surveillance Age*, N.Y. TIMES (June 7, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/2CTC-CJ33]; *see, e.g.*, Chris Kirkham & Jeffrey Dastin, *A Look at the Intimate Details Amazon Knows About Us*, REUTERS (Nov. 19, 2021, 11:35 AM), https://www.reuters.com/technology/look-intimate-details-amazon-knows-about-us-2021-11-19/ [https://perma.cc/VT9L-Q8BY].

66. Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY (last updated Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/2P5E-6DXF].

67. *Id.* (discussing various different ways in which businesses use data collected from consumers).

68. Leslie K. John, Tami Kim, & Kate Barasz, *Ads That Don't Overstep*, HARV. BUS. REV., Jan.-Feb. 2018, at 62, 62–64 (ad-targeting); Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, HARV. BUS. REV. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias?registration=success [https://perma.cc/W7XH-DKK2] (hiring); Raj Dash, Andreas Kremer, & Aleksander Petrov, *Designing Next-Generation Credit-Decisioning Models*, MCKINSEY & CO. (Dec. 2, 2021), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/designing-next-generation-credit-decisioning-models [https://perma.cc/T6Z4-WFZM] (lending); Ari Libarikian, Kia Javanmardian, Doug McElhaney, & Ani Majumder, *Harnessing the Potential of Data in Insurance*, MCKINSEY & CO. (May 12, 2017), https://www.mckinsey.com/industries/financial-services/our-insights/harnessing-the-potential-of-data-in-insurance [https://perma.cc/6ZQ4-BE7Z] (insurance).

69. *See* Tim Lau, *Predictive Policing Explained*, BRENNAN CTR. FOR JUST. (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained [https://perma.cc/S7LZ-XR46] (criminal risks); Dan Zitting, *Using Machine Learning to Predict and Detect Fraud*, FORBES (Nov. 20, 2020, 7:10 AM), https://www.forbes.com/sites/

All of these data products, both the helpful ones and the creepy ones, often use data without their users' knowledge or consent.[70] Most data collection is considered "voluntary," but most people don't truly volunteer to participate in the collection of their data.[71] Users may technically consent to providing their data by driving on public roads lined with license plate readers, by clicking "I agree" to access an online service, or by opting to live and work in buildings that require keycard access. But these choices are illusory. People must make them in order to participate in daily life.[72] People trade privacy for access to goods, services, and public participation.

The majority of Americans don't want their data to be collected, but they feel that, nowadays, it is impossible to avoid.[73] The devices and systems that collect and use people's data try to ease the public's discomfort about personal data by promising to anonymize their personal information, but even when companies promise that they will anonymize data, that data can easily be reidentified.[74] The firms that own personal data hold overwhelming power in modern society, because they control how people's data is used to make major decisions about life. Data owners can either be responsible data keepers, or they can be careless data barons that care only about profits, and not about the public's interest in their personal data.

In some cases, people's lack of control over their data endangers their civil rights.[75] Law enforcement agencies use personal data that they license from data brokers to skirt Fourth Amendment requirements and data privacy-protecting procedures.[76] In 2015, police mistakenly charged a man

---

forbestechcouncil/2020/11/20/using-machine-learning-to-predict-and-detect-fraud/?sh=30b4741a8b4b [https://perma.cc/E3GC-S7SV] (fraud); David Deming, *Balancing Privacy with Data Sharing for the Public Good*, N.Y. TIMES (Feb. 19, 2021), https://www.nytimes.com/2021/02/19/business/privacy-open-data-public.html [https://perma.cc/GT3J-824U] (public benefits).

70. *See* sources cited *supra* note 69.

71. Veronica Barassi, *Datafied Citizens in the Age of Coerced Digital Participation*, 24 SOCIO. RSCH. ONLINE 414, 415, 418 (2019).

72. *Id.* at 419; *see also* Daniel M. Filler, David M. Haendler, & Jordan L. Fischer, *Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data*, 50 CONN. L. REV. 105, 107 (2022) ("However, in many cases, individuals must surrender personal data in exchange for the basics of survival.").

73. Angela Chen, *Most Americans Think They're Being Constantly Tracked – and That There's Nothing They Can Do*, MIT TECH. REV. (Nov. 15, 2019), https://www.technologyreview.com/2019/11/15/238341/privacy-pew-research-data-collection-big-tech-facebook-google-apple/ [https://perma.cc/2GB2-TRU7].

74. Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECH CRUNCH (July 24, 2019, 5:30 AM), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ [https://perma.cc/H2ST-GVPQ] (discussing studies finding that no "anonymized" data is safe from re-identification).

75. *See* Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS (July 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights/ [https://perma.cc/DP7K-V89U].

76. Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J.

in Arkansas with murder after his friend was found dead in his hot tub.[77] Companies provided the police with data from the connected devices in his home (an Amazon Echo in his kitchen, a Nest thermostat on his wall, and his Honeywell home security system).[78] He was arrested based on his water usage data, which, according to law enforcement, showed that he washed blood from the crime scene.[79] Data-based presumptions like these lead to erroneous arrests. These erroneous criminal assessments are don't just violate people's civil rights. They also reinforce systemic racism by disproportionately including the data of Black men, who are overrepresented in law enforcement datasets.[80]

In other cases, personal data is used in ways that harm people's private rights. Mistakes in personal datasets have barred people from getting auto insurance, and even accessing their own bank accounts.[81] Beyond police and insurance companies, child welfare agencies, landlords, banks, and even hospitals use personal data dossiers containing billions of data points from thousands of sources to assess how "risky" people are as employees and parents.[82] The companies that own and have access to data dossiers "know" more about people than their family does.[83] Public institutions and private firms make decisions based on streams of medical, religious, political information, and other intimate data.[84]

The personal data analytics systems built for companies and government institutions are infused with the same biases as criminal assessment systems.[85] A reporter asked a data broker about what kind of information it sells to health insurance companies. The company's representative explained that the algorithms may process information like

---

INT'L L. & COM. REG. 595, 595-98 (2004), *cited in* Sarah Lamdan, *When Westlaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing*, 43 N.Y.U. REV. L. & SOC. CHANGE 255, 276–77 n.130 (2019).

77. Colin Dwyer, *Arkansas Prosecutors Drop Murder Case That Hinged on Evidence from Amazon Echo*, NPR (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo [https://perma.cc/84Z6-3ABS].

78. *Id.*

79. *Id.*

80. *See, e.g.*, Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/6MW7-4UUT].

81. Alice Holbrook, *When LexisNexis Makes a Mistake, You Pay for It*, NEWSWEEK (Sep. 26, 2019, 2:17 PM), https://www.newsweek.com/2019/10/04/lexisnexis-mistake-data-insurance-costs-1460831.html [https://perma.cc/7SPW-KTF9].

82. Hannah Webha-Bloch, *Transparency After Carpenter*, 59 WASHBURN L.J. 23, 23–33 (2020) (describing the kinds of information companies collect on individuals).

83. FTC REP., FISCAL YEAR 2014 AGENCY FINANCIAL REPORT, at 15 (2014).

84. Wolfie Cristl, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*, CRACKED LABS, (Jun., 2017), https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf [https://perma.cc/EJC8-WXF3].

85. *Your Data Is Shared and Sold. . . What's Being Done About It?, supra* note 46.

whether someone was "[a] high school dropout who had a recent income loss and doesn't have a relative nearby" because those people might have higher health costs.[86] When the reporter asked the data broker whether the same type of person might be healthy, the representative said, "Sure," without seeming concerned that the data could lead to erroneous health insurance decisions.[87] Assumptions, errors, and biases in datasets and data analytics systems can have serious, negative impacts on people's lives. When our data is fed through products that sell predictions to bosses, landlords, governments, and healthcare providers, the results can erroneously prevent people from obtaining housing, insurance, and even accessing their bank accounts.[88] Meanwhile, the people whose data is being bought and sold can't even see what is in their data dossiers because the companies treat their data analytics products as trade secret-protected property,[89] or they make consumers go on wild goose chases to try to find and repair data errors instead of fixing the errors in their own collections.[90]

Data ownership schemes that leave the public with little, if any, way to own or control their own data are at odds with the public's interest.[91] People want access to and control over their data use, and they want data privacy.[92] When KPMG surveyed American consumers about data responsibility in 2020, 87% of the respondents saw data privacy as a human right.[93] Without any sort of property balancing mechanism in place, there is little anyone can do to control how their data is collected and used, or even what their data dossiers contain.[94] Data companies help the government buy its way around due process obligations, and help private companies reduce people to numeric risk assessments. Data brokers are making modern risk assessment, surveillance, and policing look like the chilling worlds depicted

86. Marshall Allen, *Health Insurers Are Vacuuming up Data About You—and It Could Raise Your Rates*, NPR, https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/4RQ6-LU9Z].

87. *Id.*

88. *See* Holbrook, *supra* note 81*;* Megan Kimble, *The Blacklist*, Tex. Observer (Dec. 9, 2020), https://www.texasobserver.org/evictions-texas-housing/ [https://perma.cc/A94G-2RGJ].

89. Your Data Is Shared and Sold. . . What's Being Done About It?, *supra* note 46.

90. LAMDAN, *supra* note 1, at 38.

91. Your Data Is Shared and Sold. . . What's Being Done About It?, *supra* note 46.

92. Gabrielle Rodgers, *Consumer Wants: Privacy Transparency, Online Security, Better Customer Experience*, CMSWIRE (May. 12, 2022), https://www.cmswire.com/customer-experience/consumer-wants-privacy-transparency-online-security-better-customer-experience/ [https://perma.cc/9JHT-LAWD].

93. Macey Bayem, *87% of Americans view data privacy as a human right, but most still use risky security* practices, TECHREPUBLIC (Jul. 29, 2020, 6:00 AM), https://www.techrepublic.com/article/87-of-americans-view-data-privacy-as-a-human-right-but-most-still-use-risky-security-practices/ [https://perma.cc/P8GL-QX5M].

94. Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY (Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/4G5H-RQXR].

in the pages of dystopian novels like *1984* and *Fahrenheit 451*, and nobody can escape them by shutting the book.[95]

B. Using a Property Law Model for Digital Materials

Property law provides models for ownership and access that could be applied to personal data, but applying those models to personal data is not straightforward. People's data is different from other personal, intellectual, or real property. Unlike intellectual property, personal data is factual, not an original creation of the mind.[96] Unlike real property, data is not fixed. It is an invisible material that can zip around the world in seconds.

Personal data being viewed as a good, commodity, or saleable product is a relatively new concept.[97] Data analytics and other digital innovations have invigorated a new informational market that monetizes tidbits of personal information about every aspect of life.[98] In paper format, and without a connected internet, personal data had far less value. A physical phone book, school photo, or sales receipt had little market worth. Few companies cared to collect data about how many steps someone took each day or whose comments were liked more.

The ownership rules of this booming personal data market are still "legal grey zones."[99] Courts already enforce well-established rules for how people own, sell, and share real property and personal property (chattels), but digital property is still in flux.[100] In the 1970s, around the time that databases were mainstreamed, legal scholars were quick to dismiss the idea of treating personal data as property, calling it a "facile and legalistic" approach that would fail to "magically vest[] the powerless with control of their personal data."[101] At the time, a property law scheme for personal data never came to pass. But the idea of applying property law ideas to personal data re-emerged

95. Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment?*, WIRED (Feb. 11, 2020, 7:00 AM), https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/ [https://perma.cc/HG8A-QB8H].

96. *See* Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 19, 26 (2018) (discussing, in the context of data privacy, how intellectual property law does not protect factual information).

97. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1289 (2000) (discussing personal data as property); Schwartz, *supra* note 7, at 2057.

98. Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1374 (2017) (discussing the personal data economy).

99. Sarah Spiekermann et al., *Personal Data Markets*, Electronic Markets (Jun. 2015), https://www.researchgate.net/publication/276124405_Personal_Data_Markets [https://perma.cc/KHZ7-6YW2].

100. AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY 1 (2016); SARAH LAMDAN, DATA CARTELS 10 (2022).

101. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 211 (1971), *quoted in* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1288–89 (2000).

in the early 2000's,[102] when inventions like wireless internet (WiFi) and social media made the internet more accessible and drove more people online to share personal information.

While lawmakers have failed to safeguard people's individual data rights, companies have figured out how to bend property laws to protect their datasets and digital information troves. For instance, publishers, music labels, and movie producers have figured out how to use intellectual property concepts to protect their data property rights. They use copyright law to limit purchasers' access to ebooks, music, videos, and other types of digital content by licensing access to a streaming platform instead of selling the materials.[103] When someone uses an Amazon Kindle, Spotify's music app, or the Netflix video-streaming service, they never fully own the content they pay for. Instead, they just borrow content from the companies' data clouds and never get the First Sale rights that balance property interests between copyright holders and copy purchasers.[104]

In contrast, individuals, who have far less market power than publishers or tech platforms, have not been as successful at protecting their personal data and limiting its access and use.[105] Data companies have successfully claimed that their ownership of personal data is fair and square because they provide users with terms of service online and allow them to consent to collecting cookies and digital other data tracking.[106] (Nevermind that these terms and agreements are often obligatory click-through barriers that consumers must comply with in order to avail themselves of the digital resources they need.)

Digital apps and platforms leverage their power to gatekeep apps, platforms, and other tools that the public wants, and sometimes need, to access to hoard the entire bundle of property rights related to personal data, reserving all of the possession, control, exclusion, derivation of income, and disposition of people's data to themselves. In the digital world, non-owners have few, if any, ways to access resources that are paywalled, restricted, or otherwise unavailable online. They also have no easy way to repair or remove misinformation, even if it's about them.[107]

---

102. *See, e.g.*, Litman *supra* note 97, at 1287; Lemley *supra* note 17, at 1546; Samuelson, *supra* note 9, at 1127.

103. *See* PERZANOWSKI & SCHULTZ, *supra* note 100, at 1.

104. *Id.*

105. Stephen T. Black, *Who Owns Your Data?*, 54 IND. L. REV. 305, 316 (2021) (discussing who owns personal data).

106. Maurice E. Stucke, Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data, Harv. Bus. Rev. (Mar. 27, 2018), https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data [https://perma.cc/PJJ8-4TXJ].

107. George Krasadakis, *Fake News and Misinformation: How digital tech can help*, Innovation Mode (Oct. 28, 2022), https://www.theinnovationmode.com/the-innovation-blog/misinformation-online-a-solution-powered-by-state-of-the-art-tech [https://perma.cc/PH3U-YL7H].

When data collectors and controllers own all of the rights to people's data, individuals are stripped of their data rights, forced to agree to data-exploiting terms in order to use platforms and apps. Most people feel like they must surrender their data rights in order to use internet products and services. In the status quo, people have only a few statutorily granted rights to privacy to certain types of data.[108] For the most part, the entities that own people's data can do whatever they want with it.[109]

This one-sided ownership scheme gives the data owner full control over individuals' personal data.[110] The current personal data industry doesn't just limit data creators' rights, it reserves *no* rights for its human data producers.[111] Once personal data is collected by a third-party company, it can be sold and shared without consent.[112] After someone logs on to Facebook, they have little control over where Facebook sends their data.[113] In most jurisdictions, there are no transparency requirements obligating collectors to explain where the data is going.[114] If a user consents to handing their data over to one company by using their digital platform or app, they open the gates for other data enterprises to purchase or share, sell, and otherwise exploit their data without limits or oversight.

This scheme also lets companies exploit people's digital labor. Like intellectual property, humans create personal data.[115] However, unlike intellectual property, humans often do not choose to produce data or consensually sign over their rights to it.[116] So many companies profit from personal data that researchers have labeled users "data laborers," toiling away online to generate data for companies to monetize. Whenever someone posts on social media, buys a meal on GrubHub, or uses most other apps and services, they add valuable data to companies' troves. Datafication makes users super-producers, and their digital devices transform into personal data

108. *See What are the rights of data subjects under GDPR?*, TRUE VAULT, https://www.truevault.com/resources/compliance/what-are-the-rights-of-data-subjects-under-gdpr. [https://perma.cc/865P-MQWW] (last visited Nov. 13, 2022).

109. Stucke, *supra* note 106.

110. Stucke, *supra* note 106.

111. *Id.*

112. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, THE N.Y. TIMES (Sep. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/U9H7-25FT].

113. Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, CONSUMER REPORTS (Apr. 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook-a7977954071/ [https://perma.cc/FRS8-ZQX5].

114. Klosowski, *supra* note 112.

115. Luke Irwin, *The GDPR: What exactly is personal data?*, IT GOVERNANCE (Mar. 22, 2022), https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data [https://perma.cc/W847-VVD5].

116. Klosowski, *supra* note 112.

vectors.[117] As Karen Gregory explained in 2014, "Big Data, like Soylent Green, is made of people."[118]

In 2018, intellectual property attorney Karl Kowallis warned that digitization would tip the balance of data control towards data owners and away from the public.[119] Digital property owners have proven this warning apt by upending traditional property ownership rules.[120] In a world where companies can buy and sell your most intimate data, shouldn't *you* have some sort of say or control over that? Most people would say yes.[121] But how should we regulate personal data interests? Some data privacy advocates think that people should have complete ownership of their personal data.[122] In 2020, Congress considered a bill called the "Own Your Own Data Act," which would require social media companies to give users the ability to obtain and export their data from the platforms and license it back to the companies.[123] But this approach would create a practical mess. When the United States Court of Appeals for the Ninth Circuit considered whether people's performances featured films were copyrightable, it opined that treating individuals' appearances on film as personal property would "be a logistical and financial nightmare." This type of personal ownership would turn a "cast of thousands into a . . . copyright of thousands."[124] Giving each social media platform subscriber rights to their own personal data would have a similar effect, forcing a platform like Facebook to work with each of its almost three-billion users, individually, to secure various data rights.

If giving people full ownership of their data creates a logistical nightmare, what is a better way to divvy out the "bundle of rights" that define the relationship between data owners, purchasers, and creators? It seems we need to split that bundle, giving some rights to companies that create apps so that they can make our phones and other electronics work with ease, but reserving some rights to the people who create the data so that they can control and limit how companies use their data and fix errors in their data dossiers. A less one-sided property right, like an easement, may be the way to go. Easements create a balance between the status quo, which is outright

117. Jathan Sadowski, *When data is capital: Datafication, accumulation, and extraction*, BIG DATA & SOC'Y (Jan. 7, 2019), https://journals.sagepub.com/doi/full/10.1177/2053951718820549 [https://perma.cc/G8J5-LVNE].

118. Karen Gregory, *Big data, like Soylent Green, is made of people*, CUNY ACAD. COMMONS (Nov. 1, 2014), https://digitallabor.commons.gc.cuny.edu/2014/11/05/big-data-like-soylent-green-is-made-of-people/. [https://perma.cc/L4HJ-EXJE].

119. Karl Kowallis, *Treating Fair Use as an Easement on Intellectual Property*, 2018 BYU L. REV. 1073, 1073 (2018).

120. Paulius Jurcys et al., *Ownership of User-Held Data: Why Property Law is the Right Approach*, JOLT DIGEST (Sep. 21, 2021), https://jolt.law.harvard.edu/assets/digestImages/Paulius-Jurcys-Feb-19-article-PJ.pdf [https://perma.cc/XH6T-UBFF].

121. Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 207–8 (1890) (discussing property rights of individual's information).

122. *Id.*

123. Own Your Own Data Act, 116 S. 806 (2019).

124. Garcia v. Google, Inc., 786 F. 3d 733, 743 (9th Cir. 2015).

corporate ownership of personal data, and the opposite, giving people ownership over their own data. Something akin to an easement right of access and right to amend would balance this by giving users a few sticks from the bundle of rights.

C. Traditional Personal Ownership Will Not Create Data Equity

Even though it would be logistically tricky to grant people full personal data rights to their own data, it reflects a reasonable desire, from the public, to be more in control of its personal information. People feel a sense of ownership over their data exhaust, and many people, including lawmakers, consider their data something that *belongs* to them, which makes property law solutions an attractive way to solve data privacy problems. According to proponents of strict property law approaches like the Own Your Own Data Act, if people own their own data, they will be in control of how it is used.[125] Enterprises that wanted to use someone's data would have to buy or otherwise negotiate ways to obtain it. [126] Unauthorized use would be prohibited.[127] After all, people own their own intellectual property and decide who to sell it to: Why can't they own their own personal data?

One reason that this conceptualization of property law hasn't been adopted is that personal data is factual, and courts have declined to apply property rights to facts. When tasked with assessing whether the phone book was copyrightable,[128] the Supreme Court held that raw data, without additional original expression, is not intellectual property protected by copyright laws.[129] Facts can be used, cited, and shared by anyone.[130] The law treats factual data and information differently than creative output.[131] Copyright law only protects original works—works that are "independent creations," not borrowed—and those works must show some degree of creativity.[132] They are expressions of original ideas, not the repetition of factual information.[133]

Although imbuing data exhaust with personal property rights may sound like a simple fix in theory, assigning personal property rights to data would raise a slew of practical problems. There are good reasons that judges don't confer property rights to the information collected in phone books, databases, or our DNA.[134] Granting people property rights over the products

125. *See* Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 373 (2021).
126. *See id.* at 347–48.
127. *Id.* at 359–60.
128. Feist Publ'ns. v. Rural Tel. Serv. Co., 499 U.S. 340, 342–43 (1991).
129. *Id.* at 361.
130. *Id.* at 363–64.
131. *Id.* 347, 363.
132. *Id.* at 341.
133. *Id.* at 348.
134. Paulina Firozi, *The Health 202: The Supreme Court Banned Patenting Genes. But Congress Might Change That*. WASH. POST (Jun. 3, 2019), https://www.washington

of our human intellect—poems, plans, and ideas—is different from giving people the right to own plain facts.

One reason is that facts cannot be owned, according to property law doctrine, is because they are not original to the creator.[135] This rationale certainly applies to facts about the weather or the name of a town, but it is less applicable to personal data. Someone's blood pressure data *does* originate from within them, just as their shopping selections and dating preferences to. While it might not be creative, private data is certainly the original expression of its creator. A more logical rationale is that, if people could own their own facts, they could assert ownership over newsworthy information that may be of interest to the public. Fully conveying property rights to personal facts to their individual creators, outright, would make reporting them much more time-consuming and less efficient.[136] We need access to factual information in order to function as a society.[137]

Restricting personal data flows would also stifle productive data projects. Data can be used for social good. People trace pandemics, smooth out traffic, and plan better cities with open data collections.[138] Big data collections are uniquely able to quickly identify correlations and patterns that allowing for quick analyses that are otherwise impossible, like matching illnesses to genetic traits or predicting health outcomes based on geography.[139] Imbuing personal rights into data would also make life less convenient. Weather apps and traffic maps rely on personal data to tell people how to get places and whether to take an umbrella.[140] If users owned their data, companies would have to bargain for information with each user, one by one, interrupting the smooth flow of personal information that greases the wheels of online platforms, apps, and services.[141]

Making data into personal property could also perpetuate inequality. When people are not sure about the value of a good, they will accept whatever terms they are given, according to the phenomenon of "bounded rationality."[142] In other words, data companies have an upper hand because

---

post.com/news/powerpost/paloma/the-health-202/2019/06/03/the-health-202-the-supreme-court-banned-patenting-genes-but-congress-might-change-that/5cf1987f1ad2e52231e8e91b/ [https://perma.cc/JD6V-WYB5].

135. *Feist*, 499 U.S. at 362.

136. *See* Fracassi & Magnuson, *supra* note 125, at 347–48.

137. Laura Neuman, *A Key to Democracy: Access to Information Critical for Citizens, Governments.* The Carter Ctr. (Apr. 11, 2005), https://www.cartercenter.org/news/documents/doc1860.html [https://perma.cc/R72E-9ZHJ].

138. GOVLAB & OECD, Open Data in action, Initiatives during the initial stage of the COVID-19 pandemic (2021).

139. Radar, *What is "Alt Data", Who is Using It and Why,* Radar by Behavox (Jun. 26, 2019), https://radar.behavox.com/what-is-alt-data-who-is-using-it-and-why/ [https://perma.cc/TM6P-BW3N].

140. Carpenter v. United States, 38 U.S. 2206, 2220 (2018).

141. *See* Fracassi & Magnuson, *supra* note 125, at 348; *see also supra* text accompanying notes 134, 136.

142. Schwartz, *supra* note 7, at 2081.

nobody knows how much their data is worth. Consumers will likely accept whatever terms they are offered in personal data negotiations. Additionally, economically disadvantaged people may be pushed to sell their data even when it's not in their best interest. Data could become the new plasma—a billion-dollar industry that "depends on the blood of the very poor."[143] Just as plasma centers underpay people, giving them $30 for $300 worth of plasma, an exploitative data industry could induce cash-strapped people to sell their data for less than it's worth.[144]

Finally, turning people's data into our personal property may not be enough protection from a privacy perspective.[145] After all, intellectual property rights don't protect creators from exploitation.[146] They are regularly shaken down for their property and stripped of rights. Taylor Swift famously had to reproduce her entire catalog after the copyright holder refused to give her access.[147] Society should aspire for a higher standard of personal data protections where intimate data is concerned.

Despite these issues, data ownership is a popular idea—according to one survey, 79% of consumers believe they should be compensated when their data is shared.[148] The popularity of this desire indicates that some sort of balancing of rights is necessary.[149] People want to have more control over what happens to their data, and they want to be able to opt in to data use, rather than to serve as unwitting data producers for digitally based companies.[150] Lawmakers recognize that people should also be able to correct erroneous data about themselves, and that they should be able to have transparency about where their data is going and how it's being used.[151]

---

143. Zoe Greenberg, *What Is the Blood of a Poor Person Worth?* N.Y. TIMES (Feb. 1, 2019), https://www.nytimes.com/2019/02/01/sunday-review/blood-plasma-industry.html [https://perma.cc/BW8N-2H5K].

144. *Id.;* Luke Shaefer & Analidis Ochoa, *How Blood-Plasma Companies Target the Poorest Americans*, The Atlantic (Mar. 15, 2018), https://www.theatlantic.com/business/archive/2018/03/plasma-donations/555599/ [https://perma.cc/YJN3-34LZ].

145. Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1551 (2000).

146. Ryan Prior, *When it comes to artists losing the rights to their songs, Taylor Swift is hardly alone.* CNN (Jul. 2, 2019), https://www.cnn.com/2019/07/01/business/taylor-swift-rights-trnd [https://perma.cc/NS55-DE88].

147. *Id.*

148. Cameron F. Kerry and John B. Morris, Jr., *Why Data Ownership is the Wrong Approach to Protecting Privacy*, Brookings (Jun. 26, 2019), https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/ [https://perma.cc/J7NC-JCJD].

149. *See id.*

150. *See id.*

151. *See, e.g.*, European Data Protection Regulation (2016); Privacy Act of 1974 5 U.S.C.A. § 552a (1975) (amended 2005); California Consumer Privacy Act (2018) (all of these laws require data companies to provide their data to consumers, and to allow consumers to correct erroneous data and opt out of data collection).

D. Easements as a Model for Personal Data Ownership

Easements are a property concept meant to strike a balance between owners and non-owners in situations where important public functions are at stake.[152] They balance public interest and private ownership by giving rights to both property holders and other parties.[153] Easements could allow people to access, amend, and restrict the flow of their personal data, without conferring the responsibilities of personal data ownership onto every individual. They could strike a balance between the status quo, where corporations control our data, and the opposite extreme, where people own their data in full.

Easements, as a concept, are less rigid and more flexible for digital information, including personal data.[154] Property law does not generally allow "sole and despotic" dominion over a thing; it treats property ownership as a bundle of rights that can be split to balance interests.[155] In contrast, today's data ownership scheme *does* feel extreme and despotic, a tyrannical system where a few ruling data companies make billions of dollars by siphoning people's data and exploiting it.[156]

Easements give their holders nonpossessory, limited property interests to use another person's land.[157] Easements are intended to protect ownership, but with public interest caveats. Just as easements grant certain rights to property to non-owners, they create certain limitations for the property's owners "burdening" the property, and its possessors, with limitations and responsibilities.[158] Some common types of easements allow for utilities to run across land and provide access to natural resources that would otherwise be inaccessible or privatized.[159] In short, easements force owners to do things with their property that they wouldn't otherwise do, often for the public good.

---

152. *See, e.g.*, 4 RICHARD R. POWELL, POWELL ON REAL PROPERTY, § 34.07 (Michael Allan Wolf ed., 2022); WILLIAM B. STOEBUCK & DALE A. WHITMAN, THE LAW OF PROPERTY 449–51 (3d ed. 2000).

153. *See* 4 POWELL, *supra* note 152, § 34.07; STOEBUCK & WHITMAN, *supra* note 152, at 435–40.

154. *See* Lipton, *supra* note 22, at 175–76; *cf.* John A. Lovett, *A Bend in the Road: Easement Relocation and Pliability in the New* Restatement (Third) of Property: Servitudes, 38 CONN. L. REV. 1, 2–6 (2005) (describing rationale behind modern trend that allows more flexibility for modifications of easements).

155. *Compare* 2 WILLIAM BLACKSTONE, COMMENTARIES *2 (stating the right of property is "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe"), *with* Lucas v. South Carolina Coastal Council, 505 U.S. 1003, 1027 (1992) (explaining that states may exercise power over a landowner's "bundle of rights" through the Takings Clause).

156. *See supra* notes 110–118 and accompanying text.

157. JON W. BRUCE & JAMES W. ELY, JR., THE LAW OF EASEMENTS AND LICENSES IN LAND § 1:1, Westlaw (database updated Aug. 2022).

158. *See id.*

159. *See, e.g.*, *id.* § 1:2; 4 POWELL, *supra* note 152, § 34.01[1].

Easements are different than leases or licenses. They are also different than contract- granted rights like the ones included in data licensing agreements, which are the common tool that companies use to force people to give away their data rights.[160] Easements are property interests that exist, in many cases, no matter the contract language.[161] They can be set up as permanent, enduring access that is superior to the whims of contracting parties.[162]

As agreements go, easements are a strange formation in United States law, which strongly prefer unfettered freedom to form contracts without restraints.[163] Easements effectively interfere with that freedom, and also prevent owners from taking full advantage of their property when that property, or some of its features, are critical to the public interest or some private interest deemed socially valuable.[164] There are some social goods that are deemed so necessary to the public that policymakers decided to protect them against private property interests.[165]

Easements come in different shapes and sizes. There are a variety of ways to arrange nonposessory interests in someone else's property.[166] They can be explicit or implied.[167] Some easements (affirmative easements) give their subjects the privilege of using land they do not own in specific ways, and others (negative easements) limit how their subjects can use land they do not own.[168] Easements can be "appurtenant" and run with the property as a permanent condition of ownership, or they can be "in gross" and disappear when the property changes ownership.[169]

There are also different types of easements for different situations: easements that allow people to cross land on their way (including roads and

160. *See* BRUCE & ELY, *supra* note 157, § 1:2.

161. *See id.*

162. *See id.* §§ 1:4–1:5.

163. See id. § 1:1 ("In light of the burden easements place on landownership, why does the law recognize such a concept? The notion of freedom of contract may explain why an express easement should be enforced between the original parties to the transaction. But why should subsequent landowners be bound?"); Carol M. Rose, *Servitudes, Security, and Assent: Some Comments on Professors French and Reichman*, 55 S. CAL. L. REV. 1403, 1403–09, 1404 n.8 (1982).

164. *See* Rose, *supra* note 163, at 1403 ("[W]e tolerate these 'dead hand' arrangements because they provide a long lasting security for land development and encourage property owners to invest in the long term improvements that are essential to the productive use of real estate.").

165. These include things like providing electricity, water, and other services, and enjoying resources like waterfronts and parks. *See, e.g.*, ANGELA KALLHOFF, WHY DEMOCRACY NEEDS PUBLIC GOODS 1 (2011).

166. BRUCE & ELY, *supra* note 157, § 1:1 ("Easements are created expressly, implied in certain circumstances, established by prescriptive use, or obtained by estoppel, custom, public trust, condemnation or equity.").

167. *Id.* Easements may be implied from prior use, deed descriptions, references to a plat, acts of dedication, or necessity. *Id.* § 4:15. On the other hand, a prescriptive easement may be established by years of open, notorious, and continuous use. *Id.* § 5:2.

168. 4 POWELL, *supra* note 152, § 34.02[2][c].

169. *See id.* § 34.02[2][d].

railways), easements that allow for certain utilities, those who maintain them, to remain on a particular patch of land (electrical lines, water pipes, etc.), and easements that give people access to shared resources like waterfronts and wildlife.[170] Easements can be made to meet all sorts of needs—providing access, increasing movement, preventing certain uses.

With so many types of easements, what types could apply to personal data? Personal data easements could provide data creators with some access to view and correct their data, limit its alienability to third parties, and restrict owners from using their data in certain ways. In 2004, law professor and privacy law expert Paul M. Schwartz suggested an easement-like balancing of interests, which he called "hybrid inalienability."[171] Inalienabilities are restrictions on transferability, ownership, and use.[172] For instance, in Schwartz's scheme, a data owner could use its data but not transfer the use downstream to other data-powered entities and projects.[173] In his scheme, data collection would also be required to set an opt-in default instead of an opt-out default.[174] There would be a right of exit, where people could choose leave at any time and take their data dossiers with them.[175] There would also be an enforcement mechanism to render punishments to data companies that refuse to comply with these rules.[176] Like other property easements, Schwartz's approach balances owners' use of personal data to further technological progress, but also ensures some protections for the data subjects.[177] These types of easements—restrictions on transfer and use, rights of access, rights of exit, etc.—could be established by statute, like the fair use exception to copyright.[178]

Another easement-like statute could require data companies to give their data subjects the choice of reserving some access to their data. This access would not be full ownership like the "Own Your Own Data Act,"[179] because companies wouldn't have to cede the entirety of their ownership. Data owners would not have to hand over whole data dossier to individuals. Instead, the companies would have to allow provide limited types of access,

---

170. *See id.* § 34.11[3]–[6]; RESTATEMENT (THIRD) OF PROPERTY: SERVITUDES § 2.15, cmt. d (A. L. I. 2000).

171. Schwartz, *supra* note 7, at 2094.

172. *Id*.

173. *Id*.

174. *Id*.

175. *Id*.

176. *Id*.

177. *See id*.

178. The fair use exception balances "the interest of authors and inventors in their works" and "society's competing interest in the free flow of ideas, information, and commerce." Kowallis, supra note 119, at 1092. (quoting Gary Knapp, Annotation, *Supreme Court's Construction and Application of Limited-Times Provision in Federal Constitution's Art 1,§ 8, cl 8, Authorizing Congress to Provide "for Limited Times" Copyright and Patent Protection,*154 U.S. Sup Ct. law. Ed. 2d 1185 (2012)),

179. *See* S.806, 116th Cong. (2019), https://www.congress.gov/116/bills/s806/BILLS-116s806is.pdf [https://perma.cc/TS8T-RBCC].

use, and restrictions to people who want it. This would be similar to a fiduciary model, setting up the data owner as the caretaker of the data property but forcing it to maintain certain responsibilities to the easement holders.

One reason easements are better for people than the current terms of service agreements they click into is that, unlike contractual agreements that require assent from both sides, easements can be inferred regardless of whether an explicit contract exists.[180] Data owners would be subject to easement requirements even if they do not formally agree to them, so long as the law creates or enforces an easement.[181] In data ownership, where owners are for-profit companies that would likely prefer not to create any access to their datasets, easement-like restrictions on data could force the companies to be more open and equitable with the people whose data they're exploiting.

This easement idea for personal data runs parallel to similar arguments for easements in an intellectual property context. Copyright scholars have suggested easement-like balancing for regulating digital copyright.[182] Fair use is a statutory provision which preserves certain uses for non-owners. In certain circumstances, non-owners can copy, share, and use materials that are owned by someone else. It embraces the public interest in information access by balancing rights between the rights holder and the challenging party.[183] In a digital landscape where copyright holders have benefitted from the "copyright-as-property analogy" for decades,[184] the "fair-use-as-an-easement" analogy is seen as a way to ensure that content creators reserve some rights to use their own work.[185] Intellectual property experts see easements in a copyright context as a tool for rebalancing digital property "to strengthen the public's interest in copyrighted works" and "push back" on companies' stranglehold on informational power.[186] The problems of digital copyright access and personal data access are similar, in that companies are putting information that should be accessible to people out of those people's reach.

Although personal data easements could balance the public interest and the interests of data companies, there are still sticking points and imperfections in this property scheme.[187] While technology has changed a lot

180. Kowallis, *supra* note 119, at 1085.

181. Jason Mazzone, *Copyright Easements*, 50 AKRON L. REV. 725, 726 (2017).

182. Kowalis, *supra* note 119, at 1105; Mazzone, *supra* note 181, at 1105.

183. eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

184. *See* Kowallis, *supra* note 119, at 1074, 1086–88. *See generally* Justin Hughes, *Copyright and Incomplete Historiographies: Of Piracy, Propertization, and Thomas Jefferson*, 79 S. CAL. L. REV. 993 (2006) (providing an extensive historical overview on the copyright-property analogy).

185. *See* Mazzone, *supra* note 181, at 726–27.

186. Kowallis, *supra* note 119, at 1073.

187. In an ideal world, perhaps private data wouldn't be considered an alienable good at all. But that ship has sailed. We can't put the data-as-property cat back in the bag, even if it's not in the public interest to do so. Also, it probably isn't in the public interest to strip

since the 2000's when this idea last resurfaced, one thing that hasn't changed in the last 20 years (and that has possibly even increased) is the desire to ensure alienability for property owners.[188] Lax antitrust laws, broad permission to draw up all sorts of contract provisions, and pro-ownership court decisions in copyright and other property rulings protect and entrench the right of owners to transfer, dispose of, and otherwise treat their property as they wish.[189] Even if people have grown more concerned with creepy data collection and more open to data privacy interventions, they still support the freedom to use property as they wish, unfettered by restrictions like those included in easements.[190] In the case of data, the alienability inherent in property rights allows data owners to "freely transfer to third parties" whatever interest they acquired.[191] Limiting the interests for data owners to resell and share our data goes against that basic property law principle.

There are also practical issues inherent in personal data easement schemes. Even if the political and legal preference for alienability weren't an issue—how will policymakers set up this system? How will it be enforced? Who will pay for administration costs (and will the costs make it not worthwhile for the public interest by making the costs outweigh benefits)? Also, the structure of easements in data is not as solid as physical easements. When personal data is transferred, there is often no formal handover or receipt of sale between the data owner and the person who is giving away their data. Personal data does not come with a deed recording a transfer or rights. Its transition across users is far less formal, and usually lacks a formal, easy-to-trace record. Easements require additional administrative work to record, track, and enforce them. Property rights won't "magically vest[] the powerless with control over their personal data."[192] Policymakers can't just imbue personal data with easement rights and call it a day. In order to actually work, they have to set up a system of enforcement and redress to ensure that the easements are obeyed and respected by all of its stakeholders.

Another problem with limiting who can use data is that limiting who can access and use data could clash with First Amendment rights. There is a reason people can't own facts—the First Amendment guarantees a right to access and use information.[193] As privacy experts wrote in 1995, "The idea that one can 'own' a name or other basic identifying information raises serious First Amendment concerns."[194] To this point, courts have agreed that

---

data of its alienability because we rely so heavily on the innovations of data-fueled technologies.

188. Schwartz, *supra* note 7, at 2069.
189. *Id.* at 2074.
190. *Id.*
191. Samuelson, *supra* note 9, at 1138.
192. Litman, *supra* note 97, at 1293.
193. Lamont v. Postmaster Gen., 381 U.S. 301, 308 (1965).
194. ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 329 (1995).

facts are not property, and cannot be treated as such.[195] However, courts have not used the First Amendment to dispose of easement-like access and restrictions on personal data yet.[196] There is room to argue that property rights are not the same as privacy rights when it comes to personal data. Privacy and freedom of speech issues wound into First Amendment protections are separate from questions of data ownership, and there are ways to give people more rights to opt-in to data collection, to see and correct their data dossiers, and to have some control over their digital exhaust without interfering with the freedom of speech.[197] Defamation law has managed to splice First Amendment rights from the right to protect oneself from certain types of personally invasive speech. Similarly, legal safeguards, including the Fourth Amendment warrant process, have managed to balance privacy and the need to access personal information. Courts will have to make similar, deliberate differentiations between facts as part of speech, or as part of necessary government work, and facts as private data, as more and more personal data becomes fodder for data systems and tools. But no matter what the courts decide about personal-data-as-speech, lawmakers shouldn't hesitate to balance property interests so that personal data owners are required to protect certain rights to that data.

CONCLUSION

As personal data becomes an increasingly a valuable good extracted and used by every industry, there is a growing urgency to regulate its use in a way that balances private profit and the public's interests. Data collection and use is becoming an overwhelming, pervasive reality of daily life.[198] When Jessica Litman described the imbalance of data rights back in 2000, she described data collection as a limited practice in which "walks round the block are still unrecorded" and "interactions that begin and end and stay within the home are still largely unreported."[199] In 2022, both of those descriptions are laughably false. Neighborhood strolls aren't just tracked by video camera, they are recorded on phones, wearable devices, drones, and doorbells.[200] License plate readers track us as we drive and park our cars.[201]

---

195. U.S. News & World Report, Inc. v. Avrahami, at law No. 95-1318, in chancery No. 96-203, 1996 WL 1065557, at *6 (Va. Cir. Ct. Jun 13, 1996) (holding that the defendant "has no property right" in any of the names he falsely used in purchasing goods and services); *see also* Int'l News Serv. v. AP, 248 U.S. 215 (1918).

196. *See generally* Neil Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM & MARY L. REV. 1501 (2015).

197. J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 56, 63–72 (1997).

198. Judith Wagner DeCew, *Privacy and Its Importance with Advancing Technology*, 42 OHIO N.U. L. REV. 471, 473 (2016).

199. Litman, *supra* note 97, at 1284 (This essay summarizes prior debate and scholarship on the issue of whether personal data should be treated as property).

200. DeCew, *supra* note 198, at 473.

201. *Id.*

The interiors of homes are lined with data-collecting devices.[202] Thermostats, thermometers, stoves, and coffee makers collect personal data.[203] We even put data-collecting surveillance devices on countertops that record everything we say and do.[204]

While Lipton's digital reality is outdated, her legal suggestion that "using existing concepts in new ways enables the creation of the new theoretical framework for information law is still relevant today.[205] Real property easements, a concept over a century old, could balance the interests between humans and the companies that control and their data and treat it as their property.

Even if we agree with scholars who say that property law application is too glib and superficial for such a complex type of material, it still stands to reason that there are ideas to be borrowed from property law doctrine. Easement concepts are one of the ideas worth borrowing because easements balance property interests that are both alienable and central to the public interest.[206]

It has been suggested that using property law to grapple with data privacy issues is a bad idea, because it keeps data risk and injustices in the private realm. So long as personal data is treated like private property, subject to private contracts and private markets, people worry that it will be considered beyond the scope of public intervention and regulation.[207] I agree that property law interventions for data privacy are not as powerful as a comprehensive, federal data privacy law, but regulatory and legislative intervention is desperately needed and so far, Congress has failed to act.

Data exploitation is a sprawling problem that has spilled across industries and institutions. Just as a large battle is fought on multiple fronts, large, sprawling legal issues can be met by an array of responses. Property law concepts are another arrow in the quiver of those hunting for solutions to balance the inequities of today's data ownership realities.

202. *Id.*
203. *Id.*
204. *Id.*
205. Lipton, *supra* note 22, at 711.
206. Mazzone, *supra* note 181, at 759.
207. Litman, *supra* note 97, at 1289.