Fordham Law Review

Volume 90 | Issue 4 Article 7

2022

On the Propertization of Data and the Harmonization Imperative

Luis Miguel M. del Rosario
Fordham University School of Law

ON THE PROPERTIZATION OF DATA AND THE HARMONIZATION IMPERATIVE

*Luis Miguel M. del Rosario**

The digital age has paved the way for unforeseen and unconscionable harms. Recent experiences with security breaches, surveillance programs, and mass disinformation campaigns have taught us that unchecked data collection, use, retention, and transfer have the potential to affect everything from health-care access to national security. And they have shown the growing need for a solution that addresses this proliferation of intangible collective harms.

This Note champions data propertization—the process of establishing a bundle of rights in data comparable to those that comprise property interests—as the proper method for preventing and redressing data harms. More specifically, this Note analyzes Illinois's Biometric Information Privacy Act, California's Consumer Privacy Act, Virginia's Consumer Data Protection Act, and Colorado's Privacy Act to show that data propertization is already underway under the banner of data protection and privacy. In each case, state law advances data propertization by empowering individuals with a bundle of rights that mirror emblematic property rights to possess, exclude, and alienate, while establishing a framework for enforcement of those rights.

Notwithstanding this development, this Note also illustrates that differences between the four laws have exposed gaps in rights and enforcement, which only fragment and jeopardize data propertization. To address this issue, this Note prescribes a harmonized bundle of rights best suited to developing property interests in data and argues that those rights should be codified in federal law, dually enforced through agency enforcement and a private right of action. By eliminating gaps between existing data propertization laws and preventing the proliferation of others, such an approach would spur the development of a more cohesive and more significant property interest in data that is more capable of withstanding a new age of digital harms.

* J.D. Candidate, 2023, Fordham University School of Law; B.A., 2018, Tufts University. I would like to thank Professor Olivier Sylvain for his indispensable guidance and feedback. I am also grateful to Joe Palandrani and the staff and editors of the *Fordham Law Review* for their assistance throughout this process. Lastly, I would like to thank my family and friends for their unconditional love and support.

INTRODUCTION

Our technology knows us better than we know ourselves. On Instagram, targeted advertising so effectively predicts consumer preferences that many believed the platform was secretly recording their conversations.[1] Similarly, TikTok's video recommendations algorithm is so skilled at learning about users' interests that it seamlessly curates "For You" pages with shocking accuracy and granular specificity.[2] Google Maps, meanwhile, boasts the ability to predict traffic flows almost an hour into the future.[3] And everyday appliances equipped with Amazon Dash sensors can place an order for printer toner, coffee pods, and laundry detergent before you can even think to check how much was left.[4]

Indeed, the digital age has brought about technologies that have propelled past our wildest imaginations into fixtures of everyday, inexorable necessity. And those technologies are driven by data—the infamously abstract, catch-all term for electronic information created, collected, stored, and transferred across the digital world.[5] Engagement data powers Instagram's advertising and TikTok's recommendations engine, location data allows Google Maps to predict traffic flows, and sensor data prompts Amazon Dash–enabled appliances to place refill orders.[6] Individual pieces of this data, standing alone, may contribute little to those technologies, but in the aggregate, data plays a valuable and outsized role in the digital era. As the Organisation for Economic Co-operation and Development summarizes, "[t]he [value and] volume of data only increases with its collection and use, creating a deep well of possibility for scientific discovery and for improving existing or inventing new products and services."[7]

---

1. *See* Kaitlyn Tiffany, *The Perennial Debate About Whether Your Phone Is Secretly Listening to You, Explained*, VOX (Dec. 28, 2021, 11:50 AM), https://www.vox.com/the-goods/2018/12/28/18158968/facebook-microphone-tapping-recording-instagram-adsj [https://perma.cc/X29L-WQVW]. Instagram's CEO debunked this claim. *See Head of Instagram Adam Mosseri Sits Down for Interview with Gayle King*, CBS NEWS (June 25, 2019), https://www.cbsnews.com/video/head-of-instagram-adam-mosseri-sits-down-for-interview-with-gayle-king/ [https://perma.cc/JN9K-JKPF].

2. "One viral video laid out TikTok's communities like a treasure map: to get to the wholesome world of Frog TikTok, you had to leave Straight TikTok, find your way to Stoner Witch or Cottagecore, pass through Trans and Non-Binary, and 'go through the portal to reach the promised land.'" Abby Ohlheiser, *TikTok: Recommendation Algorithms*, MIT TECH. REV., Mar.–Apr. 2021, at 52, 52–53; *see also Inside TikTok's Algorithm: A WSJ Video Investigation*, WALL ST. J. (July 21, 2021, 10:26 AM), https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477 [https://perma.cc/L9BY-K6DC].

3. *See* Johann Lau, *Google Maps 101: How AI Helps Predict Traffic and Determine Routes*, GOOGLE (Sept. 3, 2020), https://blog.google/products/maps/google-maps-101-how-ai-helps-predict-traffic-and-determine-routes/ [https://perma.cc/Q24G-7YCU].

4. *See Amazon Dash Replenishment*, AMAZON, https://developer.amazon.com/en-US/alexa/dash-services [https://perma.cc/8YZB-QMRC] (last visited Feb. 2, 2022).

5. *See Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data [https://perma.cc/837M-ZZ93] (last visited Feb. 2, 2022) (defining "data" as "information that is produced or stored by a computer").

6. *See supra* notes 1–4.

7. ORG. FOR ECON. COOP. & DEV., DATA IN THE DIGITAL AGE (2019), https://www.oecd.org/going-digital/data-in-the-digital-age.pdf [https://perma.cc/8QPB-

But there is always a danger in having too much of a good thing. Just as data has propelled technology to new heights, its unchecked collection, retention, use, and transfer have paved the way for unforeseen and unconscionable new harms.[8] In August 2021, hackers breached T-Mobile servers and placed the sensitive data of up to one hundred million customers on sale in the dark web, exposing them to identity theft and account takeovers.[9] More ominously, a startup named Clearview AI was able to build a revolutionary facial recognition program capable of identifying strangers and "revealing not just their names but where they lived, what they did and whom they knew" by scraping over three billion user images from millions of websites.[10] And, throughout 2016, an advertising agency called Copley Advertising ran a campaign that extracted and used location data to send anti-abortion smartphone ads to whoever stepped foot in or near reproductive health clinics across the country.[11] In each of these examples, unchecked data collection by one entity—even in support of otherwise innocent activity—paved the way for abuse by another.[12]

These excesses can affect the community, too. In 2018, the Cambridge Analytica scandal showed that swaying a presidential election required little more than combing through fifty million or so Facebook profiles for demographic data and using it to "identify and target political hot buttons

YPZG]. Data is now such a critical resource that it is often called "the new oil." *See, e.g.*, *The World's Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/Q4CY-22ZA].

8. *See, e.g.*, Simon Chandler, *We're Giving Away More Personal Data than Ever, Despite Growing Risks*, VENTUREBEAT (Feb. 24, 2019, 8:35 AM), https://venturebeat.com/2019/02/24/were-giving-away-more-personal-data-than-ever-despite-growing-risks/ [https://perma.cc/5HB7-E6R6]; *see also* Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99, 103 (Philip E. Agre & Marc Rotenberg eds., 1997) ("One's privacy is now less threatened by the omniscient gaze of a centralized 'Big Brother' than by the unknown and unseen collection, matching, and profiling of transactional data, a trail of which is left by every one of us as we purchase goods, apply for services, make entertainment choices, and so on. The 'new surveillance' is decentralized, routine, [and] increasingly global . . . .").

9. *See* Brian Barrett, *The T-Mobile Data Breach Is One You Can't Ignore*, WIRED (Aug. 16, 2021, 4:44 PM), https://www.wired.com/story/t-mobile-hack-data-phishing/ [https://perma.cc/H4LV-V57X]; *see also* PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 10 (2019) ("Roughly three-in-ten Americans (28%) say they have suffered at least one of three kinds of major identity theft problems in the previous 12 months at the time of the survey").

10. Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/47YE-QSJD].

11. *See* Christina Cauterucci, *Anti-Abortion Groups Are Now Sending Targeted Smartphone Ads to Women in Abortion Clinics*, SLATE (May 26, 2016, 4:31 PM), https://slate.com/human-interest/2016/05/anti-abortion-groups-are-sending-targeted-smartphone-ads-to-women-in-abortion-clinics.html [https://perma.cc/59RZ-97EL].

12. *Cf.* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 33–39 (2015) (finding that minimizing the collection and retention of data makes data breaches less likely, reduces the potential harms of data breaches, and minimizes the risk of data being used in a way that departs from the purpose for which it was initially collected).

down to the voter level."[13] And in 2020, former President Donald Trump ignited a mini-diplomatic crisis when he sought to ban TikTok in the United States over national security concerns that the app was collecting data on American users.[14] These and similar experiences have taught us that unchecked data collection, use, retention, and transfer have the potential to affect everything from health-care access to national security. As Professor Julie Cohen notes, "The gradual but accelerating movement to informational capitalism has confronted the judicial system with two large and interrelated problems: a proliferation of asserted harms that are intangible, collective, and highly informationalized; and an unmanageably large and ever-increasing number of claimants and interests."[15]

How do we fix these issues? Some believe that no change is required because litigation and public pressure adequately cure past harms while deterring new ones.[16] Cambridge Analytica, after all, shut down after immense public scrutiny,[17] and Trump was able to force a sale of TikTok's American operations to American companies.[18] Similarly, some argue that because regulation is hardly a panacea, the technology industry should be left to regulate itself as it has for decades.[19] Indeed, in the past year alone, Apple began to require "Ask App Not to Track" buttons in apps so that users can opt out of data monitoring and sharing,[20] and Google reconfigured its

13. Hal Berghel, *Malice Domestic: The Cambridge Analytica Dystopia*, COMPUT., May 2018, at 84, 85; *see also* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/N8WU-RTEV].

14. *See* Elizabeth Lopatto, *In 2020, the Trump Administration Declared War on Dancing Teens*, VERGE (Dec. 16, 2020, 8:30 AM), https://www.theverge.com/22174704/2020-tiktok-ban-trump-administration [https://perma.cc/HMP6-QVLD].

15. JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 144 (2019).

16. *See, e.g.*, Heidi Messer, Opinion, *Why We Should Stop Fetishizing Privacy*, N.Y. TIMES (May 23, 2019), https://www.nytimes.com/2019/05/23/opinion/privacy-tech-companies.html [https://perma.cc/585Y-FHXM].

17. *See* Colin Lecher, *Cambridge Analytica Is Shutting Down*, VERGE (May 2, 2018, 2:08 PM), https://www.theverge.com/2018/5/2/17311892/cambridge-analytica-us-offices-shutting-down-facebook-scandal [https://perma.cc/9SHK-5PCZ].

18. *See* Bobby Allyn, *Trump's TikTok Deal: What Just Happened and Why Does It Matter?*, NPR (Sept. 21, 2020, 6:30 AM), https://www.npr.org/2020/09/21/915043052/trumps-tiktok-deal-what-just-happened-and-why-does-it-matter [https://perma.cc/5PKQ-D8NX]. That sale was later put on hold by President Joe Biden. *See* John D. McKinnon & Alex Leary, *TikTok Sale to Oracle, Walmart Is Shelved As Biden Reviews Security*, WALL ST. J. (Feb. 10, 2021, 5:40 PM), https://www.wsj.com/articles/tiktok-sale-to-oracle-walmart-is-shelved-as-biden-reviews-security-11612958401 [https://perma.cc/S53Z-RPHA].

19. *See* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 457–59 (2011); *see also* Cass R. Sunstein, *Paradoxes of the Regulatory State*, 57 U. CHI. L. REV. 407, 441 (1990) (noting that "regulatory programs have not always succeeded, and the paradoxes of the regulatory state have been a pervasive source of its problems").

20. *See* Brian X. Chen, *To Be Tracked or Not?: Apple Is Now Giving Us the Choice*, N.Y. TIMES (Apr. 26, 2021), https://www.nytimes.com/2021/04/26/technology/personaltech/apple-app-tracking-transparency.html [https://perma.cc/7GNP-KQP7]. This new requirement so heavily impacted companies' data collection practices that Meta, Facebook's parent company, estimated that it would cost the company $10 billion in ad revenue in 2022. *See* Coral Murphy

Chrome browser to prohibit cookies that track browsing habits.[21] Other proposals attempt to solve the issue by making data more expensive.[22] To prevent harm, one narrow proposal entails levying "data taxes" to force would-be collectors to take and use only the data they absolutely need.[23] To cure harm, other proposals prioritize punishing businesses that irresponsibly handle data with heavy fines and/or criminal prosecution.[24]

One final class of proposals seeks to empower consumers directly by establishing a property interest in data.[25] Indeed, calls for "data dignity" through ownership have grown to the point that data propertization—the process of establishing a bundle of enforceable rights in data comparable to those that comprise property interests—has become a key feature of at least one presidential campaign,[26] several private projects to create a better and more inclusive internet,[27] and the European legislative answer to the data harms problem.[28] After all, property rights naturally arise to cure issues in social organization[29] and to reverse economic externalities,[30] all while recognizing the role of ownership in natural law[31] and personal identity.[32]

Accordingly, this Note champions data propertization as the proper method for preventing and redressing data harms. In Part I, this Note

---

Marcos, *Meta Plunges and Sets Off Wall Street's Worst Drop in Nearly a Year*, N.Y. TIMES (Feb. 3, 2022), https://www.nytimes.com/2022/02/03/business/stock-market-today.html [https://perma.cc/8YPH-GWT7].

21. *See* Megan Graham, *Google Says It Won't Use New Ways of Tracking You As It Phases Out Browser Cookies for Ads*, CNBC (Mar. 3, 2021, 9:02 AM), https://www.cnbc.com/2021/03/03/google-says-it-wont-track-you-directly-in-the-future-as-it-phases-out-cookies.html [https://perma.cc/L5LC-MWJ9].

22. *Cf.* Hirsch, *supra* note 19, at 458–59 (addressing the insufficiency of self-regulation).

23. *See* Ziva Rubinstein, Note, *Taxing Big Data: A Proposal to Benefit Society for the Use of Private Information*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1199, 1238 (2021).

24. During the 2020 Democratic presidential primaries, for example, Senator Elizabeth Warren argued that "[t]ech companies shouldn't be using Americans' private information for profit." Rani Molla & Emily Stewart, *2020 Democrats on Who Controls Your Data—and Who's at Fault When It's Mishandled*, VOX (Dec. 5, 2019, 4:11 PM), https://www.vox.com/policy-and-politics/2019/12/3/20965463/tech-2020-candidate-policies-online-data-equifax [https://perma.cc/XF5Q-9WEC]. Senator Warren further suggested that the failure to protect Americans' data should be met with fines or "expand[ed] criminal liability [for] any corporate executive who negligently oversees a giant company causing severe harm to US families." *Id.*

25. *See, e.g.*, Jaron Lanier & E. Glen Weyl, *A Blueprint for a Better Digital Society*, HARV. BUS. REV. (Sept. 26, 2018), https://hbr.org/2018/09/a-blueprint-for-a-better-digital-society [https://perma.cc/FM43-5B4P]; Kenneth C. Laudon, *Markets and Privacy*, COMMC'NS ACM, Sept. 1996, at 92, 99–101; Sidi Mohamed Sidi Ahmed & Duryana Mohamed, *Data in the Internet of Things Era: The Propertization of Data in Light of Contemporary Business Practices*, 21 INT'L J. BUS. & SOC'Y 81, 91–92 (2020).

26. *See, e.g.*, *Data as a Property Right*, YANG2020, https://www.yang2020.com/policies/data-property-right/ (last visited Nov. 25, 2019) [https://perma.cc/BB6G-MCML].

27. *See, e.g.*, PROJECT LIBERTY, https://www.projectliberty.io [https://perma.cc/KZM2-ZE4A] (last visited Feb. 2, 2022); DATA DIVIDEND PROJECT, https://www.datadividendproject.com [https://perma.cc/RW9J-AWWE] (last visited Feb. 2, 2022).

28. *See infra* Part I.C.3 (discussing GDPR).

29. *See infra* notes 50–51 and accompanying text.

30. *See infra* notes 52–53 and accompanying text.

31. *See infra* note 47 and accompanying text.

32. *See infra* note 48 and accompanying text.

examines data propertization through the lens of data and property to build a coherent understanding of how the two might and should work together. Part I then provides an overview of the scholarship surrounding data propertization.

In Part II, this Note examines recent data protection and privacy laws in Illinois, California, Virginia, and Colorado to reveal the inescapable truth that data propertization is already underway. In each case, state data privacy law embraces and advances data propertization by (1) conferring a bundle of rights to data that mirror emblematic property rights to possess, exclude, and alienate and (2) establishing a framework for enforcement of those rights. Consequently, this survey of legal regimes will provide a critical illustration of the ways in which property interests are only as strong as the uniformity in the rights granted and as robust as the enforcement mechanisms designed to enforce them. Above all, Part II will illustrate that while these data privacy laws individually embrace data propertization, differences between them have exposed gaps in rights and enforcement which only fragment and jeopardize data propertization.

Part III takes this lesson and addresses the fragmentation problem by focusing on the harmonization imperative. Specifically, Part III.A argues that a successful data propertization regime requires a uniform bundle of rights and accordingly proposes a set of harmonized rights around which a property interest in data should be built. Part III.B then argues that these data property rights should be codified in federal law and dually enforced through agency enforcement and a right of private action.

I. DATA, PROPERTY, AND DATA PROPERTIZATION

This Note begins with an analysis of data propertization through the lens of data and property. Part I.A explores the unique characteristics that justify tailored protections for data. Part I.B then illustrates why property law might be well suited to providing such protection and examines how that protection can and should be maintained. Part I.C concludes with a discussion of the scholarship surrounding data propertization.

A. Data

Data is created whenever we interact with technology.[33] That is, using Google Maps to navigate creates location data detailing where we have been and how we got there,[34] just as scrolling through TikTok creates engagement data that the platform uses to attract advertisers.[35] Once created, possession of that data falls to the company that owns the technology that processes the

33. *See* Lanier & Weyl, *supra* note 25 (defining "data" as "most digital activity").

34. *See Google Maps Timeline*, GOOGLE, https://support.google.com/maps/answer/6258979 [https://perma.cc/BR4U-8CGD] (last visited Feb. 2, 2022).

35. *See* Sara Morrison, *TikTok Surprises Users by Making Personalized Ads Mandatory*, VOX (Mar. 16, 2021, 3:55 PM), https://www.vox.com/recode/22334086/tiktok-privacy-policy-personalized-ads [https://perma.cc/7XTW-GVHP].

data, rather than to the interacting party.[36] As a result, individuals cannot see the types and volume of data that they create, and most are unaware of their digital footprint and the potential for harm arising from it.[37] Most Facebook users, for example, do not know that their data can be collected outside of Facebook by entities other than Facebook through a program called Pixel.[38] To compound this problem, data is becoming more and more difficult to track in a world where international data flows are an increasingly important and prevalent part of the global economy.[39] Data knows no borders—to control it, regulators must come to terms with the fact that the expanse of data that individuals create may be larger and more diffuse than anyone may realize, expect, or wish,[40] leading to greater moral hazard concerns.[41]

Attempting to control data through the law also requires recognizing data's intangibility. As an intangible asset, data is non-rivalrous and excludable: although multiple entities can simultaneously use the same piece of data (which is thereby non-rivalrous), the right set of security protocols may prevent others from accessing that data (which is thereby excludable).[42] That excludability, however, is far from absolute: because data is intangible, there is little that can be done to prevent the proliferation of data once others gain

36. *See* Aziz Z. Huq, *Who Owns Our Data?*, BOS. REV. (Oct. 25, 2021), https://bostonreview.net/articles/who-owns-our-data/ [https://perma.cc/V4UJ-YUB2] ("[I]t is often hard to assign specific pieces of data to single individuals. The information produced by social media platforms, in particular, is often relational: it captures the flow of interactions, rather than something distinct about a single user.").

37. *See* PEW RSCH. CTR., *supra* note 9, at 27 ("Though many Americans feel their activities are being tracked, online and off, by both companies and the government, very few believe they understand what these entities are doing with the data being collected.").

38. *See* Geoffrey A. Fowler, *Facebook Will Now Show You Exactly How It Stalks You—Even When You're Not Using Facebook*, WASH. POST (Jan. 28, 2020), https://www.washingtonpost.com/technology/2020/01/28/off-facebook-activity-page/ [https://perma.cc/YQ8F-G3LX] ("It's easy to forget in the constant barrage of Zuckerberg's privacy apologies and fines, but here's the reality: Facebook keeps gathering more and more data about us, with few laws restricting how it can use it."); *see also The Facebook Pixel*, FACEBOOK, https://www.facebook.com/business/learn/facebook-ads-pixel [https://perma.cc/7XKC-5GHF] (last visited Feb. 2, 2022).

39. *See* WORLD BANK GRP., DATA FOR BETTER LIVES 237 (2021).

40. *See* Laudon, *supra* note 25, at 96 ("Large-scale databases have become so ubiquitous that individuals have no possibility of knowing all the database systems in which their personal information appears.").

41. "Moral hazard is a situation in which one party engages in risky behavior or fails to act in good faith because it knows the other party bears the economic consequences of their behavior." Greg Depersio, *What Are Examples of Moral Hazard in the Business World?*, INVESTOPEDIA (July 21, 2021), https://www.investopedia.com/ask/answers/040815/what-are-some-examples-moral-hazard-business-world.asp [https://perma.cc/X3TB-ZC9M]. Businesses that hold data may be more willing to forego security investments or adopt riskier data-handling practices to save on costs if the individuals associated with the data ultimately bear the consequences of exfiltration or theft. *Cf. infra* note 89 (noting that businesses are more likely to adopt measures that reduce the risk of data exfiltration or thefts if they bear the cost of its consequences).

42. *See* CHRISTIAN RUSCHE & MARC SCHEUFEN, ON (INTELLECTUAL) PROPERTY AND OTHER LEGAL FRAMEWORKS IN THE DIGITAL ECONOMY: AN ECONOMIC ANALYSIS OF THE LAW 12 (2018).

access to it.[43] The owner of a ring, for example, can exclude others from using it by mere virtue of possessing the physical object, whereas a credit card owner cannot exclude others from using the card beyond doing their best to prevent the dissemination of the card's number and expiration date. This tension highlights the importance of controlling data at the earliest possible stage—it would be better, after all, to prevent the dissemination of data rather than to attempt to repatriate that data and its copies once they are let loose.

B. Property

That is where property comes in. According to *Black's Law Dictionary*, "property" is "[c]ollectively, the rights in a valued resource such as land, chattel, or an intangible."[44] Under this "bundle of rights" definition of property, a property interest includes not only the rights of ownership and possession but also the rights to exclude and to alienate.[45] A property interest in land, for example, achieves much more than affirming one's ties to a parcel of land through ownership: it confers powers to dispose of the land at will and to prohibit others from accessing it.[46] This section explores how such a property interest in data might arise, how it may be expanded, and how it should be maintained.

1. Justifying Property

Property is so important that moral philosophers, political theorists, and economists extol the rise of property rights as central to the development of society and the rise of the modern state. Embracing natural law, John Locke argued that a property interest is the just result of removing something from its natural state and imbuing it with labor.[47] Similarly, Professor Margaret Jane Radin advances the view that property rights reflect one's personhood: "Most people possess certain objects they feel are almost part of themselves," objects that "are closely bound up with personhood because they are part of the way we constitute ourselves as continuing personal entities in the world."[48] Accordingly, property provides keystone relational rights through which individuals establish their identity and find their place in society.[49]

---

43. *See* Laudon, *supra* note 25, at 99 ("Once individuals lose control of information about themselves and ownership of the information, the information is then used freely by other institutions"); RUSCHE & SCHEUFEN, *supra* note 42, at 12 (describing the "information paradox," in which the seller of an intangible good must disclose the product to help the buyer arrive at a price, but cannot thereafter exclude the buyer from the product).

44. *Property*, BLACK'S LAW DICTIONARY (11th ed. 2019).

45. *See* Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions As Applied in Judicial Reasoning*, 26 YALE L.J. 710, 746 (1917).

46. *See* Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1352–54 (1993).

47. *See* JOHN LOCKE, TWO TREATISES OF GOVERNMENT AND A LETTER CONCERNING TOLERATION 111–12 (Ian Shapiro ed., 2003).

48. Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 959 (1982).

49. *See* G.W.F. HEGEL, ELEMENTS OF THE PHILOSOPHY OF RIGHT 70 (Allen W. Wood ed., H.B. Nisbet trans., 8th prtg. 2003) ("[I]t is only as owners of property that [two people] have existence . . . for each other.").

Theories based in politics and economics shift the focus away from the individual to reflect a systems-level view. While chronicling the origins of political order, Francis Fukuyama posited that "[w]hen economists talk about the rule of law, they are usually referring to modern property rights and contract enforcement."[50] That is, the state arose as property law allowed it to preempt conflict by encouraging parties to cooperate and bargain in formalized and orderly markets.[51] Then, as production functions and market values began to change, property rights proved malleable in that they provided a dynamic mechanism for reducing economic externalities as they arose.[52] According to Professor Harold Demsetz, property rights systematically emerge "when the gains from propertization outweigh the costs of securing those rights."[53]

These justifications for property differ, but none are mutually exclusive of the others. A property interest in land, for example, would arise under Locke's view by virtue of the possessor's labor on it,[54] under Professor Radin's view as an extension of the owner's ties to the land,[55] and under Demsetz's view as a way to maximize the growing benefits of varied land use.[56] Similarly, a property interest in data can be justified under Locke's view as the result of an individual's interactions with technology;[57] under Professor Radin's view as a way to recognize the digital extension of an individual's identity;[58] and under Demsetz's view as a way to eradicate the harms of free access to data, which in aggregate now outweigh the costs of propertization.[59]

2. Expanding and Maintaining Propertization

But how does property law accommodate such a transition from property in land to property in data? With land, traditional property interests flow

50. FRANCIS FUKUYAMA, THE ORIGINS OF POLITICAL ORDER: FROM PREHUMAN TIMES TO THE FRENCH REVOLUTION 248 (2011).

51. *See* Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 8–10 (1960) (arguing that, absent transaction costs, private bargaining in the allocation of resources use can overcome initial entitlements). *See generally* Stergios Skaperdas, *Cooperation, Conflict, and Power in the Absence of Property Rights*, 82 AM. ECON. REV. 720 (1992) (exploring the likelihood of cooperation or conflict in the absence of property rights).

52. *See* Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 350 (1967).

53. Steven H. Hazel, *Personal Data as Property*, 70 SYRACUSE L. REV. 1055, 1056 (2020).

54. *See supra* note 47 and accompanying text.

55. *See supra* note 48 and accompanying text.

56. *See supra* notes 52–53 and accompanying text.

57. *See supra* notes 33–35 and accompanying text.

58. *See* Tyler Reigeluth, *Why Data Is Not Enough: Digital Traces as Control of Self and Self-Control*, 12 SURVEILLANCE & SOC'Y 243, 249 (2014) ("[O]ur identities are collections of digital traces"); Russell Belk, *Extended Self and the Digital World*, CURRENT OP. PSYCH., Aug. 2016, at 50, 50 (noting that current digital worlds "extend our identity beyond our mind and body alone").

59. *See supra* note 53 and accompanying text.

seamlessly because every parcel is unique, rivalrous, and excludable.[60] Physical occupation of land by one necessarily leads to exclusion of all others, and alienation necessarily involves only that discrete parcel. Intangibles like data, meanwhile, are easily duplicated, non-rivalrous, and non-excludable.[61] Thus, even if propertization established ownership, a property interest in data would mean very little if other rights in the bundle were not strong enough to prevent others from taking that data.[62] If the novel property interest is to survive the transition from propertizing tangibles to propertizing intangibles, it therefore follows that the bundle of rights must be reconfigured.[63] New rules are needed precisely because physical property rights are fundamentally different from data property rights and cannot sufficiently protect against a new category of the associated intangible harms.

In so doing, crafting a strong right to exclude is essential because it lies at the core of every property interest.[64] In the case of data, "the strength of an owner's right to exclude must reflect the strength of the privacy interest she seeks to protect"[65] because determining the appropriate scope of property protection requires taking privacy interests into account.[66] In other words, a property interest in data would require a strong right to exclude in the first instance because it encapsulates an individual's digital personhood and therefore implicates a strong privacy interest.[67] The strength of the right to exclude can thereafter be adjusted to reflect a spectrum of privacy interests in different types of data.[68]

---

60. *See* Ellickson, *supra* note 46, at 1322 ("Private property conventionally refers to a regime in which no more than a small number of persons have access to a resource."); James Chen, *Private Good*, INVESTOPEDIA, https://www.investopedia.com/terms/p/private-good.asp [https://perma.cc/BL4N-5AVU] (Jan. 5, 2021) (defining "private goods" as "rivalrous and excludable").

61. *See supra* notes 42–43 and accompanying text.

62. *Cf.* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609, 615 (1962) ("[T]here is a fundamental paradox in the determination of demand for information; its value for the purchaser is not known until he has the information, but then he has in effect acquired it without cost. Of course, if the seller can retain property rights in the use of the information, this would be no problem.").

63. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."); Demsetz, *supra* note 52, at 354–59 (discussing examples where property interests must shift to accommodate shifting externalities); *see also* Laudon, *supra* note 25, at 102 ("Property law is quite flexible in recognizing value in a variety of tangible and intangible assets . . . .").

64. *See, e.g.*, Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 744 (1998) ("[I]f we start with the right to exclude, it is possible with very minor clarifications to derive deductively the other major incidents that have been associated with property."); *see also* Abraham Bell & Gideon Parchomovsky, *The Privacy Interest in Property*, 167 U. PA. L. REV. 869, 916 (2019).

65. Bell & Parchomovsky, *supra* note 64, at 916.

66. *Id.* at 920.

67. *See supra* note 58; *supra* note 48 and accompanying text.

68. *See* Warren & Brandeis, *supra* note 63, at 215 ("Any rule of liability adopted must have in it an elasticity which shall take account of the varying circumstances of each case . . . ."). Indeed, empirical data suggests that Americans place varying degrees of importance on keeping data private, depending on the type(s) and purpose(s) for which it is

Similarly, bailments[69] in data must come with a duty of care so that entities who possess others' data are made responsible for the costs of potential harm.[70] This duty of care must likewise remain flexible depending on the privacy interest at stake: it may require nothing more than the adoption of responsible data-handling practices,[71] or it may be strict to the point of requiring "information fiduciaries" to affirmatively act in data owners' best interests.[72] In either case, a bailor's scope of consent is necessarily central to what bailees may do with borrowed data, when they can do it, and to what extent they may do it.[73]

Once the metes and bounds of a property interest are established, monitoring whether individuals respect or violate others' property rights is key to maintaining the underlying interest because property is a law of relations.[74] Where a right in one creates a duty in another, protecting a property interest requires not only the preservation of rights but also the corroboration that duties correlative to those rights are adequately

collected. *See* Venky Anant et al., *The Consumer-Data Opportunity and the Privacy Imperative*, MCKINSEY & CO. exhibit 2 (Apr. 27, 2020), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative [https://perma.cc/R8K4-LFWJ]; PEW RSCH. CTR., *supra* note 9, at 34.

69. A bailment is "[a] delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose, usu[ally] under an express or implied-in-fact contract." *Bailment*, BLACK'S LAW DICTIONARY (11th ed. 2019).

70. *See* JEAN TIROLE, ECONOMICS FOR THE COMMON GOOD 404 (Steven Rendall trans., 2017) ("In general, any company that collects data should be at least partly responsible for any harmful use subsequently made of it by others, whether they obtained it directly or indirectly."); *see also* PEW RSCH. CTR., *supra* note 9, at 4 ("[M]ajorities of the public are not confident that corporations are good stewards of the data they collect.").

71. Many organizations that specialize in data storage offer responsible data handling guides. *See, e.g.*, *Data Privacy Best Practices for Organizations*, IRON MOUNTAIN, https://www.ironmountain.com/resources/general-articles/d/data-privacy-best-practices-for-organizations [https://perma.cc/3PJD-38BG] (last visited Feb. 2, 2022); *Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy*, IAPP, https://iapp.org/resources/article/big-data-security-and-privacy-handbook-100-best-practices-in-big-data-security-and-privacy/ [https://perma.cc/JRM2-3UZK] (last visited Feb. 2, 2022).

72. *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1209 (2016). *But see* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019) (arguing that establishing information fiduciaries would create more problems than it purports to solve).

73. *See* Benito Arruñada, *Property Enforcement as Organized Consent*, 19 J.L. ECON. & ORG. 401, 404 (2003) ("When the law enforces a right as a right *in rem*, consent of the right holder is required for the right to be affected, that is, damaged, in any way."); *see also* Laudon, *supra* note 25, at 99 ("Privacy invasion occurs whenever personal information of any kind is obtained and used without the consent of the individual."); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559, 598 (2015) ("Data gathering, aggregation, categorization, and subsequent disclosure to third parties . . . may be perceived as an invasion of our privacy because the subsequent actions taken with our data violate the expectations we had of the behavior of third parties in whom we entrusted our data.").

74. *See* Abraham Bell & Gideon Parchomovsky, *A Theory of Property*, 90 CORNELL L. REV. 531, 544–45 (2005) ("[Hohfeld] . . . elucidated that the crux of property is not a relationship between a person and an object, as Blackstone had suggested, but rather a nexus of legal relationships among people regarding an object.").

performed.[75] Violations must therefore be corrected in actions brought by the state to enforce the interest itself,[76] or in actions brought by private individuals to enforce their moral rights.[77] Note that these avenues for correction serve distinct yet complementary goals: state enforcement corrects societal harms by enforcing property interests in explicit terms at the lowest cost,[78] whereas private enforcement allows individuals to seek redress for moral wrongs without resorting to self-help[79] or ceding control of relief.[80] A property interest is therefore only as strong as the enforcement mechanisms designed to protect it.[81]

C. Data Propertization

Having explored data propertization through the lens of data and property, this Note now turns to a discussion of the scholarship surrounding data propertization as a concept in its own right. Would it effectively prevent and cure data harms?

1. The Case for Data Propertization

Some say yes. Nobel Prize–winning economist Jean Tirole advises that the "acceptability of digitization depends on us believing that our data will not be used against us, [and] that the online platforms we use will respect the terms of our contract with them."[82] In other words, digitization "is based on

75. *See* Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions As Applied in Judicial Reasoning*, 23 YALE L.J. 16, 31 (1913) (describing duty as the "invariable correlative" of right).

76. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1090 (1972) ("Having made its initial choice, society must enforce that choice. Simply setting the entitlement does not avoid the problem of 'might makes right'; a minimum of state intervention is always necessary."); Bell & Parchomovsky, *supra* note 74, at 560 ("[I]n most cases, the enforcement of property rights is a public good that the state should centrally provide.").

77. *See* Andrew S. Gold, *A Moral Rights Theory of Private Law*, 52 WM. & MARY L. REV. 1873, 1907 (2011) ("Because the state frequently requires individuals to give up their extra-legal enforcement rights, the state provides a private right of action . . . for the plaintiff to enforce her moral rights.").

78. *See* Bell & Parchomovsky, *supra* note 74, at 561–62.

79. *See* Gold, *supra* note 77, at 1907–08.

80. *See id.* at 1912.

81. *See, e.g.*, Merrill, *supra* note 64, at 733 ("Given that property is a norm, there is also a consensus that property cannot exist without some institutional structure that stands ready to enforce it."); Bell & Parchomovsky, *supra* note 74, at 555 ("Without enforcement, one's status as owner has little independent meaning."); Arthur L. Corbin, *Rights and Duties*, 33 YALE L.J. 502, 518 (1924) ("Inasmuch as the existence of jural right and duty means nothing except that organized society affords a systematic remedy or remedies through its judicial and its executive or administrative officers, legislative action that abolishes all remedy and all sanction also abolishes the right and the duty.").

82. TIROLE, *supra* note 70, at 402.

trust."[83] And yet, a look back at the harms in this Note's introduction shows that mere trust cannot prevent harm.[84]

The case for data propertization holds that creating property rights in data would preempt the trust issue by narrowing choice and empowering consumers. It forces parties to work around clear property entitlements such that when data belongs to the individual, collectors must work around that owner's preferences and priorities to gain access to it.[85] As a result, owners' "attention will be guided by their self-defined interests rather than by manipulative platforms beholden to advertisers or other third parties."[86] Uniformity breeds empowerment, too: coherence and consistency in data propertization regimes may save individuals from an endless barrage of privacy policies by allowing them to assert an enduring say in the fate of their data wherever they go.[87] Meanwhile, a property interest in data would force businesses to more carefully adhere to the duties that attach to data in their possession so that they do not become the subject of costly enforcement actions.[88] As a result, data propertization paves the way for increased security investments that reduce the likelihood of breaches[89] such that individuals can worry less about potential harms downstream.[90]

Most importantly, data propertization is arguably the most effective avenue for preventing data harms and correcting them if they occur anyway. Though property's first-order goal is to promote consensual transactions and prevent trespass,[91] the law provides remedies for harm if it occurs anyway.[92]

---

83. *Id.*; *see also* Waldman, *supra* note 73, at 561 ("[W]hat makes expectations of privacy reasonable are expectations of trust.").

84. *See* Hirsch, *supra* note 19, at 458 (noting that, according to critics of self-regulation, "self-regulatory standards will inevitably prove too lenient").

85. *See* Calabresi & Melamed, *supra* note 76, at 1092 ("An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller . . . . [This form of entitlement] lets each of the parties say how much the entitlement is worth to him, and gives the seller a veto if the buyer does not offer enough.").

86. Lanier & Weyl, *supra* note 25; *see also* WILLIAM L. LANDES & RICHARD A. POSNER, THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY LAW 22 (2004) ("Markets and property rights go hand in hand. Property rights provide the basic incentives for private economic activity and the starting point for transactions whereby resources are shifted to their most valuable use.").

87. *See* Hazel, *supra* note 53, at 1075 ("[T]he specific rights in the bundle do not matter . . . . What does matter is that the *same* bundle always accompanies personal data. So long as data subjects understand that standard bundle, they will rarely need to examine privacy policy language. As a result, data subjects would understand the property interest transferred when they use websites—without reviewing hundreds of privacy policies.").

88. *See* Gianclaudio Malgieri, *"Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?*, J. INTERNET L., Nov. 2016, at 3, 6 ("If personal data is 'paid' for by data users, companies may be incentivized to turn more attention to protecting personal data from data breach or negligent disclosure.").

89. *See* TIROLE, *supra* note 70, at 404 ("Companies do invest large sums in online security to avert reputational damage, but would invest much more if they fully internalized the cost of such security breaches to their customers.").

90. *See supra* note 41 and accompanying text.

91. *See supra* notes 50–51 and accompanying text.

92. *See supra* notes 74–81 and accompanying text.

Judge Guido Calabresi and Professor Douglas Melamed argue that where prospective property rules fail to prevent harm, court-imposed liability-rule injunctions can cure them.[93] And when party price determinations under a property rule and injunctive relief under a liability rule prove insufficient to cure harm, Professor Paul Schwartz argues that damages awards should be made available, too.[94] With strong, harmonized entitlements[95] and robust avenues for relief,[96] data propertization stands ready to protect data on all fronts.[97]

2. The Case Against Data Propertization

On the other side of the coin, the case against data propertization dismisses the solution as too costly.[98] For example, propertization requires systematic and costly publication of the interest so that others are aware that it exists.[99] Moreover, the costs of notice and of negotiating and obtaining consent for each transaction may far exceed the potential benefits of possessing the

93. *See* Calabresi & Melamed, *supra* note 76, at 1093 ("It should be clear that most entitlements to most goods are mixed. Taney's house may be protected by a property rule in situations where Marshall wishes to purchase it [and] by a liability rule where the government decides to take it by eminent domain . . . ."); *id.* at 1092 n.7 (arguing that property entitlements that require excessive state intervention become too costly to enforce via property rules and will eventually be enforced by easily administered liability rules instead).

94. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2108–09 (2004).

95. *See supra* notes 63–73 and accompanying text.

96. *See supra* notes 74–81 and accompanying text.

97. *See* Warren & Brandeis, *supra* note 63, at 211 ("The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested.").

98. *See, e.g.*, Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 43 (2018) ("New property rights in data are not suited to promote better privacy or more innovation or technological advances, but would more likely suffocate free speech, information freedom, science, and technological progress."). Under Demsetz's theory of propertization, a property right will not arise if its costs outweigh its benefits. *See* Demsetz, *supra* note 52, at 348.

99. *See* Arruñada, *supra* note 73, at 412 (arguing that exchanges of property must be publicized so the interest remains enforceable against potential future buyers and lenders); Schwartz, *supra* note 94, at 2098 (noting that a critical condition of data propertization is "that third parties must be able to verify that a given piece of personal information has in fact been propertized and then identify the specific rules that apply to it"); Lanier & Weyl, *supra* note 25 (noting that "manag[ing] data provenance, access, and flow [is] the first step in managing its value").

data.[100] At least one economist argues that this increase in transaction costs can counterproductively weaken the property interest in the long run.[101]

Other critics emphasize that data propertization would hamper value creation and the free flow of information,[102] as granting expansive rights to exclude erroneously assumes that individuals get no value for data they provide. That assumption is unfounded, they argue: "[B]usinesses can often argue that they have spent money to acquire our data" because "[w]e provide our personal data in exchange either for useful services (search engines, social networks, instant messaging, online video, maps, email) or in the course of a commercial transaction (as in the case of Uber and Airbnb)."[103] In reality, we are not Spotify or Facebook's customers but their transacting partners in exchanges where we obtain valuable services by paying for them with our data.[104] Those who are unaware of this dynamic and prevent companies from accessing their data anyway undermine long-established practices—to put it harshly, consumers may not deserve a property interest in their data because they are ignorant of or do not care about how their data is exchanged and monetized in the first place.[105]

Lastly, justice-seeking critics note that data propertization would lead to commodification that exploits those who have no choice but to "click away rights to data in exchange for convenience, free services, connection,

100. LARRY DOWNES, A RATIONAL RESPONSE TO THE PRIVACY "CRISIS" 19 (2013) ("Transaction costs higher than the value of the transaction put an end to the hopes for a market for any kind of property, private or otherwise."). *But see* Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. INFO. POL'Y 37 (2019) (noting that critics of notice-and-consent regimes "say little about the value of notice" and arguing that "[w]e ought to decouple notice from consent, and imagine notice serving other normative ends besides readying people to make informed consent decisions").

101. *See* Carmine Guerriero, *Property Rights, Transaction Costs, and the Limits of the Market* 4 (Quaderni DSE, Working Paper No. 1110, 2021) ("[P]roperty rights are optimally weakened when transaction costs are sizable and more so the larger are the impediments to negotiation."). *But see* Laudon, *supra* note 25, at 103 ("Under a regime in which individuals own their personal information, transaction costs may rise but only as far as necessary to pay for the cost of invading privacy.").

102. *See, e.g.*, Cameron F. Kerry & John B. Morris, Jr., *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, BROOKINGS INST. (June 26, 2019), https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/ [https://perma.cc/K27W-YEWM] ("Treating personal information as property to be licensed or sold may induce people to trade away their privacy rights for very little value while injecting enormous friction into free flow of information.").

103. TIROLE, *supra* note 70, at 408.

104. *See* Will Oremus, *Are You Really the Product?*, SLATE (Apr. 27, 2018, 5:55 AM), https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html [https://perma.cc/X4JX-4LYH].

105. *See* Kerry & Morris, *supra* note 102 ("The current notice-and-choice model is failing because it is effectively impossible for users to understand either how their data will be used or the accompanying privacy risks, especially in the constant flow of online engagement in today's connected world."); Schwartz, *supra* note 94, at 2078 ("Consumer ignorance leads to a data market in which one set of parties does not even know that 'negotiating' is taking place. Even if there is a sense that some personal data are collected, many individuals do not know how or whether this information is further processed and shared.").

endorphins or other motivations,"[106] if not incentivize entrepreneurial litigation that would flood the courts with unmeritorious claims.[107] These concerns are all valid, but unfortunately, the discussion of whether to propertize data has long expired: in the European Union and in some jurisdictions in the United States, data propertization is already underway.

3. Data Propertization 101: The European Union's General Data Protection Regulation

The European Union kickstarted the process of data propertization with its 2016 data protection and privacy law, the General Data Protection Regulation (GDPR).[108] Though it flies under the banner of data protection and privacy, GDPR advances data propertization by conferring a bundle of rights in data that mirror the property rights to possess, exclude, and alienate. Specifically, the right to possess is furthered by GDPR's grant of a consumer right to be informed of and access collected data,[109] the right to exclude is furthered by GDPR's right to erasure and right to restrict processing,[110] and the right to alienate is furthered by GDPR's right to data portability.[111] Violations of these rights are then punishable by the imposition of costly administrative fines.[112] As recommended earlier, GDPR advances data propertization by granting property-based rights[113] and backing them up with robust enforcement.[114]

When it passed, GDPR was celebrated as "an ambitious achievement" set to become "the privacy lodestar for the foreseeable future."[115] Commentators cite to the law as a prime example of the "Brussels Effect," a process of regulatory globalization through which the EU "externalize[s] its laws and regulations outside its borders."[116] In other words, although EU

106. Christopher Tonetti & Cameron F. Kerry, *Should Consumers Be Able to Sell Their Own Personal Data?*, WALL ST. J. (Oct. 13, 2019, 9:00 AM), https://www.wsj.com/articles/should-consumers-be-able-to-sell-their-own-personal-data-11570971600 [https://perma.cc/2HH6-VB5S]; *see also* Kerry & Morris, *supra* note 102 ("Basing privacy protection on property systems, on the other hand, would reduce privacy to a commodity, double down on a transactional model based on consumer choice, and be enormously complicated to implement."); Laudon, *supra* note 25, at 101–02 ("[S]ome people will sell their privacy, the poor more than the rich.").

107. *See infra* note 247 and accompanying text.

108. Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

109. *See id.* arts. 13–15.

110. *See id.* arts. 17–19.

111. *See id.* art. 20.

112. *What Are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines/ [https://perma.cc/ZFQ8-Q9SW] (last visited Feb. 2, 2022).

113. *See supra* notes 63–73 and accompanying text.

114. *See supra* notes 74–81 and accompanying text.

115. Jennifer Dumas, *General Data Protection Regulation (GDPR): Prioritizing Resources*, 42 SEATTLE U. L. REV. 1115, 1127 (2019); *see also* Anant et al., *supra* note 68 (calling GDPR "a bellwether for data-privacy regulation").

116. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3 (2012). The Brussels Effect is a spin-off of the California Effect, a term coined by David Vogel to describe the state's ability to set strict consumer and environmental regulation standards for the entire

regulations technically only apply to member states, they are nonetheless so expansive in applicability that they effectively impose EU law on other countries such as the United States.[117] In the next part, this Note will illustrate that data protection and privacy laws in the United States adopt a similar approach to data propertization, leading to distinct and novel standard-setting effects.

II. DATA PROPERTIZATION IN THE UNITED STATES

The inescapable truth is that data propertization is already underway in the United States. In this part, an examination of state privacy laws will show that the process of data propertization has already begun in Illinois, California, Virginia, and Colorado under the banner of data protection and privacy. An analysis of each state's data protection regime will highlight three important lessons. First, like with GDPR, the bundle of rights granted under each law establishes a property interest in data because they mirror the emblematic rights to possess, exclude, and alienate that together make up traditional property interests. Second, this property interest—no matter how strong or expansive the ensuing rights may be—is only as strong as the enforcement mechanisms designed to protect it. Third, and most importantly, while data privacy laws in Illinois, California, Virginia, and Colorado individually embrace data propertization, differences between the four laws have exposed gaps in rights and enforcement, which only fragment and jeopardize data propertization writ large.

A. Illinois: The Biometric Information Privacy Act

Illinois embraced GDPR's rights-heavy model of data propertization a full decade before GDPR came into effect, and it did so with one of the first laws in the United States to respond to the new age of data harms. The Illinois Biometric Information Privacy Act (BIPA),[118] unanimously passed in 2008,[119] was a landmark law enacted to protect consumer biometric data[120] through increased regulation.[121] BIPA was the Illinoisan response to the uneasiness and anger that arose when private entities went bankrupt without indicating whether they would delete or sell off the data in their

United States. *See id.* at 5; DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 248–70 (1995).

117. *See generally* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019).

118. *See* 740 ILL. COMP. STAT. 14/1–99 (2021).

119. *See* 2008 Ill. Laws 3693; *Biometric Information Privacy Act (BIPA)*, ACLU ILL., https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa [https://perma.cc/3V5H-TNJ6] (last visited Feb. 2, 2022).

120. BIPA specifically protects "biometric identifiers," which are defined as including "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILL. COMP. STAT. 14/10 (2021).

121. *See id.* 14/5(g) ("The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.").

possession.[122] By establishing a bundle of rights to an individual's biometric data and imposing duties upon entities that deal with that data, BIPA effectively establishes a property interest in biometric data. As the Illinois chapter of the American Civil Liberties Union asserts: "A person's biometric information belongs to them, and only them."[123]

1. Rights and Duties

BIPA recognizes the irreversibility of trespassory data harms[124] by placing the right to exclude at the very center of the property interest in biometric data.[125] Specifically, section 15(b) prohibits the collection, capture, purchase, and receipt of another's biometric data without their informed consent.[126] This gatekeeping exclusion is further bolstered by section 15(c), which wholly prohibits the subsequent sale, lease, and trade of biometric data.[127] Under section 15(d), even a profitless disclosure or dissemination of data requires separate consent.[128] Through a default blanket prohibition on the use of others' biometric data, these provisions empower data owners to assert the value of their data and regulate its use on their own terms.[129]

But the duties do not end there. Where sections 15(b), (c), and (d) establish direct duties between owners and collecting entities, sections 15(a) and (e) impose general duties that collecting entities owe to all data owners.[130] Section 15(a) imposes a duty on all entities that retain, collect, or disclose biometric data to publicly disclose a policy that "establish[es] a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied."[131] In the meantime, section 15(e) requires entities to "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry."[132] These duties effectively restrict collecting entities to activities within an owner's original

122. *See* Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1098 (N.D. Ill. 2017).

123. *See Biometric Information Privacy Act (BIPA)*, *supra* note 119.

124. *See* 740 ILL. COMP. STAT. 14/5(c) (2021) ("[S]ocial security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.").

125. *See supra* notes 64–68 and accompanying text.

126. *See* 740 ILL. COMP. STAT. 14/15(b) (2021); *id.* 14/10 (defining the requisite "[w]ritten release" as "informed written consent").

127. *Id.* 14/15(c).

128. *Id.* 14/15(d).

129. *See supra* note 85; Schwartz, *supra* note 94, at 2103 ("An opt-in rule forces the data processor to obtain consent to acquire, use, and transfer personal information. It creates an entitlement in personal information and places pressure on the data collector to induce the individual to surrender it.").

130. For more on the distinction between duties owed to specific people and those owed to an indefinite class, see Hohfeld, *supra* note 45, at 718.

131. 740 ILL. COMP. STAT. 14/15(a) (2021).

132. *Id.* 14/15(e)(1).

scope of consent[133] and impose a requirement that they act as responsible custodians of the biometric data in their possession,[134] thus reducing moral hazard concerns.[135]

2. Enforcement

BIPA concretizes these rights through strong enforcement mechanisms. Under section 20, any prevailing party "aggrieved by a violation" of the law can obtain, "for each violation," up to $1000 in liquidated damages for a negligent violation and up to $5000 for an intentional or reckless violation.[136] Although BIPA allows prevailing plaintiffs to recover actual damages,[137] the baseline availability of liquidated damages creates a strong incentive for businesses to adhere to BIPA's provisions at all costs since plaintiffs—now theoretically free from the burden of proving actual damages to recover—may find it easier to litigate these claims.[138]

This dynamic led to "one [of] the largest settlements ever for a privacy violation" in *In re Facebook Biometric Information Privacy Litigation*.[139] In that case, plaintiffs alleged that, as part of its "Tag Suggestions" photo program, Facebook collected and stored user facial scans without notice or consent, thus violating BIPA sections 15(a) and 15(b).[140] Rather than go to trial, the parties agreed to a $650 million settlement that put "at least $345 into the hands of every class member interested in being compensated."[141] Facebook additionally agreed to turn its facial recognition features off by default globally, to publicly disclose how it intends to use facial data moving forward, and to delete all existing and stored facial data for class members who did not opt in to the feature.[142] BIPA thus paved the way for the plaintiffs to be directly compensated for the alleged harms and more broadly forced the allegedly violating party to comply with the law moving forward. In short, BIPA served to compensate for past harms and to prevent new ones all in one go.[143]

---

133. *See supra* note 73 and accompanying text. For example, BIPA would prevent bankrupt companies from selling off biometric data in their possession to satisfy creditors. *See supra* note 122 and accompanying text.

134. *See supra* notes 69–72 and accompanying text.

135. *See supra* note 41.

136. 740 ILL. COMP. STAT. 14/20 (2021).

137. *See id.*

138. *See* Schwartz, *supra* note 94, at 2083 ("Permitting liquidated damages . . . encourages litigation, the specter of which may deter infringements of privacy. It will also allow others who are not parties to the litigation to benefit from improved privacy practices that follow successful litigation.").

139. 522 F. Supp. 3d. 617, 620 (N.D. Cal. 2021).

140. *See id.* at 621.

141. *Id.* at 620.

142. *See id.* at 622.

143. Facebook ultimately announced on November 2, 2021, that it would shut down its facial recognition software entirely. *See* Jerome Pesenti, *An Update on Our Use of Face Recognition*, META (Nov. 2, 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/ [https://perma.cc/KX8W-9HNK].

Indeed, the strength of BIPA's design has only been confirmed by the litigation it enabled. In *Rosenbach v. Six Flags Entertainment Corp.*,[144] the Illinois Supreme Court issued a landmark decision in which it ruled that state claims under BIPA did not require a concrete and individualized injury in fact to survive a motion to dismiss.[145] According to the court, only a technical, textual injury in law was required to maintain a cause of action because "[t]o require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse . . . would be completely antithetical to the Act's preventative and deterrent purposes."[146] This ruling led to an explosion in BIPA claims driven by plaintiffs eager to assert their newfound property interests in biometric data.[147]

3. Moving Forward

BIPA's provisions methodically establish a property interest in biometric data by defining biometric data as a discrete object, vesting a bundle of rights in that data, and providing a mechanism for enforcing those rights. The strength of this design has led to what may well become the "Illinois Effect" in data regulation.[148] BIPA litigation has already cropped up across the country, tackling technologies that use biometrics to unlock devices[149] or to identify race, gender, and ethnicity.[150] If BIPA litigation continues on its trajectory,[151] it is likely that private entities will take a greater initiative to honor their data obligations to protect individuals' biometric data.[152]

---

144. 129 N.E. 3d 1197 (Ill. 2019).

145. *Id.* at 1207.

146. *Id.*

147. *See* Sara Merken, *Surge in Biometric Privacy Suits Causes Firms to Boost Specialty*, BLOOMBERG L. (Mar. 14, 2019, 4:45 AM), https://news.bloomberglaw.com/business-and-practice/surge-in-biometric-privacy-suits-causes-firms-to-boost-specialty [https://perma.cc/PHT8-VJVA].

148. *See supra* notes 115–17 and accompanying text.

149. *See generally* Complaint, Barnett v. Apple, No. 2021CH03119 (Cook Cnty. Cir. Ct. Ill. June 25, 2021); Celeste Bott, *Apple Hit with Biometric Suit over Products' ID Features*, LAW360 (June 30, 2021, 7:51 PM), https://www.law360.com/articles/1399198/apple-hit-with-biometric-suit-over-products-id-features [https://perma.cc/54JP-45EB].

150. *See generally* Third Amended Class Action Complaint, Vance v. Int'l Bus. Machines Corp., No. 20-cv-00577 (N.D. Ill. Jan. 24, 2020); Complaint, Vance v. Microsoft Corp., No. 20-cv-01082 (W.D. Wash. July 14, 2020).

151. This trajectory is far from guaranteed. A recent pair of bills before the Illinois legislature proposes BIPA amendments that would gut the law by weakening its core features and superseding landmark district court and state court interpretations thus far. *See ACLU Warns That Illinois Privacy Rights at Risk This Week*, ACLU ILL. (Mar. 8, 2021, 7:15 AM), https://www.aclu-il.org/en/news/aclu-warns-illinois-privacy-rights-risk-week [https://perma.cc/L6GG-8JJ3].

152. *See supra* note 138; *see also* Michael McMahon, Note, *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts*, 65 ST. LOUIS U. L.J. 897, 939–40 (2021) ("Especially in class action suits that can add up to actual and meaningful penalties (or, at least, large settlements) for companies that use biometrics, BIPA's monetary penalties may spur such companies to be more careful in their biometric collection and use."). Alternatively, those who prefer not to enact such measures can opt out of dealing in biometric data entirely. For example, "[o]ne practical effect

B. California: The California Consumer Privacy Act

Next in the data propertization story is the California Consumer Privacy Act (CCPA).[153] Like BIPA, CCPA was enacted in response to a data crisis—this time the Cambridge Analytica scandal.[154] When it unanimously passed in 2018,[155] it was heralded as "one of the most significant regulations overseeing the data-collection practices of technology companies in the United States."[156] California voters took this legacy one step further in November 2020, when they approved Proposition 24 to enact the California Privacy Rights Act (CPRA),[157] which strengthened key features of CCPA by amendment.[158] This section will show that, both in its original and as-amended forms, CCPA takes a substantial step toward propertizing a wider range of data through a more comprehensive set of rights and duties.

1. Rights and Duties

CCPA creates property interests in a wider swath of data than BIPA by covering all "[p]ersonal [i]nformation," which is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[159] The law only contains exceptions for data that is publicly available,[160] anonymized or aggregated,[161] or regulated by federal law.[162] Indeed, it goes so far as to grant property interests in data such as social security numbers,[163] email addresses,[164] records of products or

---

of BIPA is that Google's Nest security cameras do not offer in Illinois a feature for recognizing familiar faces." Shira Ovide, *The Best Law You've Never Heard Of*, N.Y. TIMES (Feb. 23, 2021), https://www.nytimes.com/2021/02/23/technology/the-best-law-youve-never-heard-of.html [https://perma.cc/A9WQ-YUV6].

153. *See* CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2021).

154. *See supra* notes 13, 122 and accompanying text; Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1781–84 (2021); Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [https://perma.cc/PX4H-G98J].

155. *See* 2018 Cal. Stat. 1807; Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill [https://perma.cc/6TZS-XGFP].

156. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/HH85-EV8A].

157. *See* 2020 California Proposition 24 (approved Nov. 3, 2020).

158. *See* Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS INST. (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/ [https://perma.cc/DD52-4MCT].

159. CAL. CIV. CODE § 1798.140(o)(1) (West 2021). Compare this with BIPA, which only protects biometric data. *See supra* note 120.

160. *See id.* § 1798.140(o)(2).

161. *See id.* § 1798.140(o)(3).

162. *See id.* § 1798.145(c).

163. *See id.* § 1798.140(o)(1)(A).

164. *See id.*

services purchased,[165] internet activity,[166] and inferences that may be drawn from that data.[167] CCPA furthers data propertization by coupling this broad coverage with a set of six rights that mirror the traditional property rights of possession, exclusion, and alienability.

Beginning with possessory rights, CCPA confers Californians with a right to know and a right to access.[168] Under section 110, data collection is subject to a consumer's right to know—that is, seek disclosure of the types and specific pieces of data collected, sources from which they were collected, and the purposes for such collection.[169] Section 115, in turn, subjects the subsequent sale or disclosure of data to a third party to a consumer's right to know the categories of data sold and the categories of third parties involved.[170] In all cases, CCPA requires that consumers have a right to access the specific pieces of data collected,[171] limits data collection to its original stated purpose unless notice is provided,[172] and prohibits the sale of data by third parties unless a consumer has been given notice and an opportunity to opt out of that sale.[173] These primary rights—to know and to access—function as possessory rights in data in that they identify the data in which the property interest lies, then consolidate ownership into a controlled, finite set by limiting any further collection, sale, or disclosure.[174]

The next two rights—the right to delete and the right to opt out—are exclusionary rights. Under section 105, businesses must comply with consumer requests to delete consumer data.[175] Similarly, section 120(a) empowers consumers to preemptively opt out of the sale and sharing of their

165. *See id.* § 1798.140(o)(1)(D).
166. *See id.* § 1798.140(o)(1)(F).
167. *See id.* § 1798.140(o)(1)(K).
168. *See id.* § 1798.100(a).
169. *See id.* § 1798.110(a).
170. *See id.* § 1798.115(a).
171. *See id.* §§ 1798.110(a)(5), 1798.100.
172. *See id.* § 1798.100(b).
173. *See id.* § 1798.115(d).
174. *See supra* notes 42–43 and accompanying text (discussing the necessity of preventing the uncontrolled proliferation of data).
175. *See* CAL. CIV. CODE § 1798.105(c) (West 2021).

data to third parties.[176] Save for a few exceptions,[177] these rights enable consumers to enforce property interests in their data by excluding others from possession.[178] Note, however, that consumers are still not able to wholly opt out of collection in the first instance. In contrast with BIPA, CCPA does not impose an informed consent regime and allows businesses to collect and use data as long as they disclose the nature of that collection and use.[179] CPRA amended CCPA to establish greater protections for "sensitive" personal information,[180] but even those protections only allow consumers to limit the use of sensitive personal information to an enumerated set of "business purpose" uses.[181] Nevertheless, by granting a more encompassing set of exclusionary rights to a narrow category of sensitive data, CCPA's dual categorization recognizes that trespasses to certain types of data lead to a greater degree of harm and thus warrant a greater degree of protection.[182] But beyond this narrow exception, CCPA's propertization regime generally vests the initial entitlement in the collecting business rather than in consumers, and exclusion only occurs when consumers later choose to take affirmative steps to protect their digital property.[183]

The final duo of rights are alienability rights flowing from the rights to portability and nondiscrimination. Section 100(d) provides the first by requiring businesses to deliver requested data "in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance."[184] Section

176. *See id.* § 1798.120(a) (effective Jan. 1, 2023). CCPA's original opt-out right only protected against the sale of consumer data. *See* 2018 Cal. Stat. 1807, 1811. CPRA extended the opt-out right to exclude the sharing of data and address a loophole whereby entities could disregard a consumer's opt-out choice by essentially delaying payments for data. More specifically, the loophole allowed companies to sell data to third parties by charging them for advertising based on that data rather than the data itself—that is, by charging for the service instead of the product itself. *See* Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019, 1:29 PM), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345 [https://perma.cc/9PGB-CXLZ] ("Facebook stated its data collection qualified for the law's exemption for sending data to 'service providers' and didn't count as a 'sale' of data under the law"). Because CPRA defines "sharing" broadly to the point of covering any type of transfer, *see* CAL. CIV. CODE § 1798.140(ah)(1) (West 2021) (effective Jan. 1, 2023), its opt-out right closes that loophole and empowers consumers to place a more encompassing bar on derivative transfers of their data.

177. *See* CAL. CIV. CODE § 1798.105(d) (West 2021).

178. *See supra* notes 64–68 and accompanying text.

179. *Compare* 740 ILL. COMP. STAT. 14/15(b) (2021), *with* CAL. CIV. CODE §§ 1798.100(b), 1798.130 (West 2021).

180. *See* CAL. CIV. CODE § 1798.140(ae) (West 2021) (effective Jan. 1, 2023) (defining "[s]ensitive personal information").

181. *See id.* §§ 1798.135(f), 1798.140(e) (effective Jan. 1, 2023).

182. *See supra* notes 65–68 and accompanying text.

183. This is only the case for data regarding adults. Known as the right to opt in, section 120(c) imposes a special restriction on the sale and sharing of data on children younger than sixteen years old: a business must receive the affirmative consent of the consumer (or their parents, in the case of children younger than thirteen years old) before engaging in such activity. *See* CAL. CIV. CODE § 1798.120(c) (West 2021) (effective Jan. 1, 2023).

184. *Id.* § 1798.100(d).

125, in turn, protects consumer choice through a right to nondiscrimination, which prohibits businesses from denying, charging different prices or rates for, or otherwise providing a different level or quality of, goods or services to any consumer who chooses to exercise any rights under CCPA.[185] A news website that collects browsing data on its users, for example, may not block access to its articles if an individual chooses to opt out of the sale of that data to third parties.[186] These two final rights protect a consumer's alienation decisions and accordingly complete the bundle of rights inherent in CCPA.

2. Enforcement

But of course, a property interest is only as strong as the enforcement mechanisms that serve to protect it.[187] In this regard, CCPA starts out strong: on the front end, CCPA protects property interests by prospectively invalidating contract provisions that "waive or limit" the rights it establishes, reasoning that such a bargain would be "contrary to public policy."[188] On the back end, CCPA protects those property rights through a robust regulatory framework that clarifies and reinforces businesses' obligations under the law.[189] For example, CCPA requires businesses to establish and maintain processes through which consumers can submit CCPA requests,[190] but it is the law's implementing regulations that provide guidance on how to process consumer requests,[191] enumerate the types of notice that must be provided,[192] and lay out the exact elements of a CCPA-compliant privacy policy.[193]

More significantly, CCPA establishes an agency entrusted with actively administering the law.[194] The California Privacy Protection Agency has powers to promulgate, revise, and implement regulations interpreting CCPA,[195] as well as the authority to conduct hearings, subpoena witnesses, compel testimony, and impose fines for violations of CCPA.[196] The agency is also tasked with ensuring that regulated businesses perform regular

185. *See id.* § 1798.125(a).

186. CCPA's right to nondiscrimination includes a notable exception under which businesses may discriminate by "offer[ing] a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data." *Id.* § 1798.125(b)(1). This is known as the "Spotify exception" because the music streaming service provides a free tier paid for by targeted advertising. *See* Lapowsky, *supra* note 155.

187. *See supra* notes 74–81 and accompanying text.

188. CAL. CIV. CODE § 1798.192 (West 2021) (effective Jan. 1, 2023).

189. *See generally* CAL. CODE REGS. tit. 11, § 999.300–999.337 (2021).

190. *See* CAL. CIV. CODE § 1798.130(a)(1)(A)–(B) (West 2021).

191. *See* CAL. CODE REGS. tit. 11, §§ 999.312, 999.313, 999.315, 999.316, 999.318, 999.323–999.325 (2021).

192. *See, e.g.*, *id.* § 999.305 (notice at collection); *id.* § 999.306 (notice of the right to opt out); *id.* § 999.307 (notice of a financial incentive); *id.* § 999.332 (notices to consumers under sixteen years old).

193. *See id.* § 999.308.

194. *See* CAL. CIV. CODE § 1798.199.10 (West 2021).

195. *Id.* § 1798.199.40(b).

196. *Id.* §§ 1798.199.55(a), 1798.199.65.

cybersecurity audits and submit security risk assessment reports.[197] By its terms, CCPA requires that the agency is comprised of members most qualified to administer the law.[198]

Yet what CCPA gave in the way of administrative enforcement, it took away in the availability of a private right of action.[199] Under CCPA, a private right of action only arises when "nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."[200] Maintaining a private right of action therefore requires not only a specialized type of security breach but also proof that the business's poor security procedures and practices enabled it. Moreover, a private cause of action is only available if the aggrieved party provides the business with notice of the alleged violation and with thirty days to cure it, a mechanism that effectively establishes a safe harbor.[201] Lastly, where CCPA establishes administrative penalties of up to $7500 per intentional violation or up to $2500 per all other violations,[202] it only permits individuals to recover up to $750 per consumer per incident in private actions.[203] With these limitations, CCPA distinguishes itself from BIPA's approach to data propertization in that it grants broader rights for the price of narrower enforcement mechanisms.

3. Moving Forward

CPRA bound CCPA to data propertization because it expressly requires that all future amendments be "consistent with and further the purpose and intent of [the] act."[204] What remains to be seen, however, is how CCPA as amended will play out on the ground: CPRA took effect on December 16, 2020, but administrative enforcement by the California Privacy Protection Agency does not begin until July 1, 2023.[205] With CCPA compliance costs expected to be as high as $55 billion statewide,[206] CCPA's success will

197. *Id.* § 1798.185(a)(15).

198. *See id.* § 1798.199.10(a) ("[A]ppointments [to the agency's board] should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.").

199. *Cf.* Kerry & Chin, *supra* note 158 ("[A]ny passable federal privacy law . . . is likely to require a more robust private right of action.").

200. CAL. CIV. CODE § 1798.150(a)(1) (West 2021). Compare this with BIPA, which provides a private cause of action even absent an injury in fact. *See supra* notes 144–47 and accompanying text.

201. *See* CAL. CIV. CODE § 1798.150(b) (West 2021).

202. *See id.* § 1798.155(b). Compare these penalty maximums with those set by BIPA. *See supra* notes 136–38 and accompanying text.

203. *See id.* § 1798.150(a)(1)(A).

204. 2020 California Proposition 24, § 25.

205. *See* CAL. CIV. CODE § 1798.185(d) (West 2021).

206. BERKELEY ECON. ADVISING & RSCH., STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS 11 (2019); *see also* Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law [https://perma.cc/72YJ-MJJ2] (noting that businesses

depend on the success of efforts to enforce it.[207] CCPA's limited private right of action[208] already effectively establishes an injury-in-fact requirement not present in BIPA.[209] As a result, Californians will lack a direct method for seeking redress for CCPA violations, and the burden of enforcing data property interests will fall on the agency.[210]

Notwithstanding these issues, CCPA embodies a return to the "California Effect": California is expected to become the standard-bearer in all matters data property and privacy, as CCPA is expected to be widely applicable and substantially impactful.[211] Although CCPA provides for limited avenues for private enforcement, it nonetheless makes a substantial step in the data propertization story because it grants a larger scope of property rights protected by the state. At the very least, "CCPA's legacy may not be the law itself, but the laws it inspires."[212]

C. Virginia: The Consumer Data Protection Act

Next in the story of data propertization is Virginia's Consumer Data Protection Act[213] (VCDPA), signed into law by Governor Ralph Northam on

---

dealing in data must "either reform their global data protection and data rights infrastructures to comply with California's law, or institute a patchwork data regime in which Californians are treated one way and everyone else another. That last option can be more expensive for companies").

207. *See supra* notes 74–81 and accompanying text.

208. *See supra* note 200 and accompanying text.

209. *See supra* notes 144–47 and accompanying text; Rahman v. Marriott Int'l, Inc., No. SA CV 20-00654, 2021 WL 346421, at *2 (C.D. Cal. Jan. 12, 2021) ("[I]n order for Plaintiff's claims to survive Defendant's motion [to dismiss], the unauthorized access of personal information on its own, without the access of further sensitive information, must be sufficient to establish injury in fact"). Some have argued that the injury-in-fact requirement prevents the law from adequately protecting individuals and allowing them to seek redress for harms. *See, e.g.*, COHEN, *supra* note 15, at 146–47 ("[T]he injury-in-fact inquiry enshrines a distinctively neoliberalized conception of the judicial role in which courts function principally to discipline deviations from marketplace norms rather than to correct more systematic marketplace excesses. That stance foregrounds harms that are discrete, individuated, and preferably monetizable . . . [but] positions more diffuse, systematic market and sociotechnical dynamics as presumptively normal—an approach that is calculated to leave most complaints about accountability for economic activity at the courthouse door."); *see also* Warren & Brandeis, *supra* note 63, at 205 ("[I]f privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting.").

210. Proposed solutions to this problem have so far failed. For example, a California bill that would have actively granted a broader private right of action failed to garner sufficient support. *See* Press Release, ACLU of N. Cal., California Legislature Caves to Big Tech Pressure Again and Undermines Consumer Privacy Rights (May 16, 2019), https://www.aclunc.org/news/california-legislature-caves-big-tech-pressure-again-and-undermines-consumer-privacy-rights [https://perma.cc/B5B7-35UV].

211. *See supra* note 116; Chander et al., *supra* note 154, at 1737 ("California has emerged as a kind of privacy superregulator, catalyzing privacy law in the United States").

212. Sara Morrison, *California's New Privacy Law, Explained*, VOX (Dec. 30, 2019, 6:50 PM), https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained [https://perma.cc/68JM-CQD5]; *see also* Chander et al., *supra* note 154, at 1787–88.

213. *See* VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2021) (effective Jan. 1, 2023).

March 2, 2021.[214] The Virginia legislature did not unanimously pass VCDPA as Illinois's did with BIPA[215] and as California's did with CCPA,[216] but the law nonetheless benefited from broad legislative support in that identical versions of the bill passed in each chamber.[217] When it passed, VCDPA became only the second privacy law in the nation following CCPA,[218] but it was the third law of its type, following BIPA and CCPA, to further data propertization. VCDPA furthers data propertization because it mirrors BIPA and CCPA in the rights and enforcement mechanisms that it establishes.[219] However, key differences between BIPA's, CCPA's, and VCDPA's reporting requirements,[220] opt-out rights,[221] and enforcement mechanisms[222] will begin to reveal the dangers of overlapping state data propertization regimes.

1. Rights and Duties

VCDPA takes a cue from CCPA by vesting property interests in a large swath of data,[223] with exceptions for data that is de-identified or publicly available,[224] if not otherwise regulated by federal law.[225] Moreover, like CCPA, VCDPA's broad definitional coverage is complemented by grants of possessory rights (the right to know[226] and the right to access[227]), exclusionary rights (the right to delete[228] and the right to opt out[229]), and alienability rights (the right to portability[230] and the right to nondiscrimination[231]). Finally, like CCPA, VCDPA protects these rights by imposing a duty to limit the data processing to initially disclosed purposes,[232] maintain reasonable data security practices,[233] and conduct regular security

214. *See* 2021 Va. Acts 35; 2021 Va. Acts 36; Cat Zakrzewski, *Virginia Governor Signs Nation's Second State Consumer Privacy Bill*, WASH. POST (Mar. 2, 2021, 8:17 PM), https://www.washingtonpost.com/technology/2021/03/02/privacy-tech-data-virgina/ [https://perma.cc/A72Q-ZXSA].

215. *See supra* note 119 and accompanying text.

216. *See supra* note 155 and accompanying text.

217. *See* H.B. 2307, 1st Spec. Sess. (Va. 2021); S.B. 1392, Reg. Sess. (Va. 2021).

218. *See* Zakrzewski, *supra* note 214.

219. *See infra* Part II.C.1.

220. *See infra* note 235 and accompanying text.

221. *See infra* notes 236–39 and accompanying text.

222. *See infra* Part II.C.2.

223. *See* VA. CODE ANN. § 59.1-575 (2021) (effective Jan. 1, 2023) (defining "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable natural person.").

224. *See id.*

225. *See id.* § 59.1-576(C).

226. *See id.* §§ 59.1-577(A)(1), 59.1-578(C).

227. *See id.* § 59.1-577(A)(1).

228. *See id.* § 59.1-577(A)(3).

229. *See id.* § 59.1-577(A)(5).

230. *See id.* § 59.1-577(A)(4).

231. *See id.* § 59.1-578(A)(4).

232. *See id.* § 59.1-578(A)(2).

233. *See id.* § 59.1-578(A)(3).

assessments.[234] In these respects, VCDPA serves almost as a jurisdictional expansion of CCPA by replicating the rights that CCPA establishes.

Emphasis on "almost." Indeed, VCDPA is perhaps more interesting in the ways in which it deviates from CCPA. For example, under CCPA, businesses must prepare regular security assessments covering their "processing of personal information" broadly, but under VCDPA, businesses need only detail targeted advertising, sales, profiling, sensitive data processing, and any processing that presents a heightened risk of harm to consumers.[235] Similarly, a consumer who opts out of data processing under VCDPA only thereafter prevents businesses from selling that data, using it for targeted advertising, or using it for "profiling in furtherance of decisions that produce legal or similarly significant effects."[236] It does not, by contrast, prevent those businesses from otherwise sharing that data—a common practice banned by CCPA's right to opt out.[237] This limitation is further entrenched by VCDPA's definition of a data "sale," which covers only "the exchange of personal data for monetary consideration."[238] Compare this with CCPA, which extends the definition of a "sale" to "other valuable consideration" and accordingly empowers an individual to opt out of equally valuable nonmonetary exchanges.[239]

But not all of VCDPA's deviations from CCPA render it more restrictive in its approach to data propertization. Taking a cue from CCPA, VCDPA defines a set of data deemed "sensitive,"[240] and taking a cue from BIPA, requires businesses to obtain a consumer's informed consent before businesses can process such data.[241] And although VCDPA defines sensitive data more narrowly than CCPA does,[242] VCDPA's opt-in right creates a stronger property right in those types of data than does CCPA by providing a stronger right to exclusion.[243] Given these differences, the Virginian property interest in data is weaker than its Californian counterpart in some respects (for example, through its limited definition of a sale),[244] yet stronger in others (for example, through its opt-in right).[245]

234. *See id.* § 59.1-580.

235. *Compare* CAL. CIV. CODE § 1798.185(a)(15)(B) (West 2021), *with* VA. CODE ANN. § 59.1-580 (2021) (effective Jan. 1, 2023).

236. VA. CODE ANN. § 59.1-577(A)(5) (2021) (effective Jan. 1, 2023).

237. *See supra* note 176.

238. VA. CODE ANN. § 59.1-575 (2021) (effective Jan. 1, 2023).

239. CAL. CIV. CODE § 1798.140(t)(1) (West 2021); *see also supra* note 176.

240. *See* VA. CODE ANN. § 59.1-575 (2021) (effective Jan. 1, 2023) (defining "[s]ensitive data").

241. *See id.* § 59.1-578(A)(5); *id.* § 59.1-575 (defining "[c]onsent as "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement").

242. For example, CCPA includes social security numbers as well as "[t]he contents of a consumer's mail, email, and text messages" in its definition of "sensitive personal information," but VCDPA does not. *Compare* CAL CIV. CODE § 1798.140(ae)(1) (West 2021), *with* VA. CODE ANN. § 59.1-575 (2021) (effective Jan. 1, 2023).

243. *See supra* notes 64–68 and accompanying text.

244. *See supra* notes 236–39 and accompanying text.

245. *See supra* notes 240–43 and accompanying text.

2. Enforcement

Unlike CCPA, VCDPA is unequivocal in its state-centric approach: the state attorney general has exclusive authority to enforce the law.[246] Thus, there is no administering agency and no private right of action under VCDPA, and the law's sponsors justify these decisions by arguing that they prevent opportunistic plaintiffs and lawyers from "'turn[ing] this into another business' by creating opportunities for lots of lawsuits."[247] Moreover, VCDPA establishes not just a narrow avenue for enforcement but also wide latitude for the regulated: the law codifies a safe harbor permitting businesses to avoid litigation if they correct alleged violations of the law within thirty days.[248] With this in mind, it is difficult to see just how effective VCDPA will be in allowing private individuals to seek redress for data harms and enforce their moral rights to property.[249] Although VCDPA largely adopts CCPA's approach to establishing broad data property rights, it concurrently peels back on the enforcement methods needed to protect them, leading to weaker property interests overall.[250]

3. Moving Forward

VCDPA does not go into effect until January 2023,[251] so its full impact will not be known until Virginian consumers and businesses try their hands at interpreting the law. A work group established under VCDPA[252] recently published a report outlining recommendations on how to address the law's shortcomings,[253] but whether and to what extent those recommendations will be adopted remains to be seen. For now, all that is clear is that VCDPA selectively mimics, but does not mirror, CCPA's approach to data

246. VA. CODE ANN. § 59.1-584(A) (2021) (effective Jan. 1, 2023).

247. Gopal Ratnam, *Virginia Set to Become Second State to Pass Data Privacy Law*, ROLL CALL (Feb. 16, 2021, 6:00 AM), https://www.rollcall.com/2021/02/16/virginia-set-to-become-second-state-to-pass-data-privacy-law/ [https://perma.cc/29MY-CFFR] (quoting statement of Senator David Marsden).

248. VA. CODE ANN. § 59.1-584(B) (2021) (effective Jan. 1, 2023). Compare this with CCPA, which provides a safe harbor for private actions but not administrative ones. *See supra* note 201 and accompanying text.

249. *See supra* notes 76–81 and accompanying text.

250. The lack of robust enforcement mechanisms led pro-privacy groups to lobby Virginia lawmakers to "hit the brakes on [the] bill." Hayley Tsukayama, *Virginians Deserve Better Than This Empty Privacy Law*, ELEC. FRONTIER FOUND. (Feb. 12, 2021), https://www.eff.org/deeplinks/2021/02/virginians-deserve-better-empty-privacy-law [https://perma.cc/P55Q-MHN9]; *see also Group Letter Opposing Weak Industry-Backed Privacy Bill in Virginia*, U.S. PUB. INT. RSCH. GRP. (Feb. 16, 2021), https://uspirg.org/resources/usp/group-letter-opposing-weak-industry-backed-privacy-bill-virginia [https://perma.cc/4MDZ-EVED].

251. *See* 2021 Va. Acts 35, § 4; 2021 Va. Acts 36, § 4.

252. *See* 2021 Va. Acts 35, § 2; 2021 Va. Acts 36, § 2.

253. *See* JOINT COMM'N ON TECH. & SCI., VIRGINIA CONSUMER DATA PROTECTION ACT WORK GROUP: 2021 FINAL REPORT (2021), https://rga.lis.virginia.gov/Published/2021/RD595/PDF [https://perma.cc/Z8VF-9DX6]. Some notable suggestions from the report include removing the right to cure from the law "to prevent companies from exploiting this provision" and reconsidering the law's definitions for "sale." *Id.* at 2.

propertization, while taking some aspects from BIPA to fill existing statutory gaps.

D. Colorado: The Colorado Privacy Act

Completing the quartet of American data privacy legislation is the Colorado Privacy Act (CPA),[254] signed into law by Governor Jared Polis on July 7, 2021.[255] Like CCPA and VCDPA, CPA advances data propertization by conferring key rights in a broad swath of data covered by the law.[256] By its very terms, the law seeks to prevent "[t]he unauthorized disclosure of personal information and loss of privacy [which] can have devastating impacts."[257] Although similar prefatory language does not exist in either CCPA or VCDPA,[258] CPA functions similarly to BIPA, CCPA, and VCDPA in bolstering consumers' bundles of rights in their data in an effort to protect them from data harms.

1. Rights and Duties

CPA adopts the now-familiar formula of granting possessory rights (the right to know and the right to access[259]), exclusionary rights (the right to delete[260] and the right to opt out[261]), and alienability rights (the right to portability[262]) in a bundle. CPA also takes a cue from VCDPA and strengthens the property interest in sensitive data with an informed consent requirement.[263] Lastly, like BIPA, CCPA, and VCDPA, CPA imposes exacting duties on businesses to minimize and limit data processing and collection to "reasonably necessary" purposes not exceeding the original intended scope of the activity.[264] CPA's prefatory language doubles down

254. *See* COLO. REV. STAT. §§ 6-1-1301 to 6-1-1313 (2021) (effective July 1, 2023).

255. *See* 2021 Colo. Sess. Laws 3445, 3467; *see also* Webb McArthur & Dailey Wilson, *Colorado Governor Signs Nation's Third Comprehensive Consumer Data Privacy Law*, AM. BAR ASS'N (Aug. 16, 2021), https://www.americanbar.org/groups/business_law/publications/blt/2021/08/data-privacy/ [https://perma.cc/39B9-96K7].

256. *See* COLO. REV. STAT. § 6-1-1303(17) (2021) (effective July 1, 2023) (defining "personal data" as "information that is linked or reasonably linkable to an identified or identifiable individual"); *id.* § 6-1-1304(2)–(3) (listing exceptions).

257. *Id.* § 6-1-1302(a)(V).

258. For similar language in BIPA, see *supra* notes 121, 124.

259. CPA collapses the right to know into the right to access. *See id.* COLO. REV. STAT. § 6-1-1306(b) (2021) (effective July 1, 2023).

260. *Id.* § 6-1-1306(d).

261. *Id.* § 6-1-1306(a)(I).

262. *Id.* § 6-1-1306(e).

263. *Id.* § 6-1-1308(7); *see also id.* § 6-1-1303(5) (defining "[c]onsent" as "a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement"); *supra* notes 241–43 and accompanying text (VCDPA). CPA largely mimics VCDPA's definition of "sensitive data" but narrows it further by excluding precise geolocation data. *Compare* COLO. REV. STAT. § 6-1-1303(24)(a) (2021) (effective July 1, 2023), *with* VA. CODE ANN. § 59.1-575 (2021) (effective Jan. 1, 2023).

264. *See, e.g.*, COLO. REV. STAT. § 6-1-1304(4)(a) (2021) (effective July 1, 2023) ("Personal data . . . [s]hall not be processed for any purpose other than a purpose expressly listed . . . or as otherwise authorized"); *id.* § 6-1-1308(3) ("A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in

on this duty of care with reference to businesses as mere "custodians" of consumer data: "By enacting [CPA], Colorado will be among the states that empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate."[265]

But CPA differs from both CCPA and VCDPA in two notable respects. First, CPA does not grant consumers with a right to nondiscrimination, thereby exposing consumers who exercise their data property rights to lower quality or more expensive goods and services, even when the difference is not at all related to the value of the consumer's data. News organizations would therefore be prohibited from blocking access to their articles if Californians or Virginians chose to exclude the companies from using their biometric data, but not if Coloradoans were to do the same thing.[266]

Second, consumers who opt out of the processing of their data under CPA can only prevent a business from selling their data, using it for targeted advertising, or using it for "[p]rofiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[267] As a result, when an opt-out right is exercised, a business must refrain from a wider set of activities in California than in Virginia and Colorado[268] but may concurrently discriminate against Colorado consumers in price or quality but not against those in California or Virginia.[269] Though the rights granted under CPA generally advance data propertization and generally mirror CCPA and VCDPA, differences between BIPA, CCPA, and VCDPA not only lead to consumer uncertainty about the strength and extent of their new property rights to data but also to interstate differences in consumer treatment.

2. Enforcement

CPA further distinguishes itself with a novel approach to enforcement. For example, CPA does not establish an agency tasked with enforcing the new law (unlike CCPA)[270] nor does it allow for a private right of action[271] (unlike

relation to the specified purposes for which the data are processed."); *id.* § 6-1-1304(4)(b) ("Personal data . . . [s]hall be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the specific purpose or purposes listed . . . or as otherwise authorized"); *id.* § 6-1-1308(4) ("A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.").

265. *Id.* § 6-1-1302(c)(I); *see also supra* notes 69–73 and accompanying text.

266. Both CCPA and VCDPA grant a right to nondiscrimination. *See supra* notes 185–86, 231 and accompanying text.

267. COLO. REV. STAT. § 6-1-1306(a)(I) (2021) (effective July 1, 2023). This mirrors VCDPA's model. *See supra* notes 236–37 and accompanying text.

268. *Compare supra* note 176 and accompanying text (describing California's broad opt-out right), *with supra* notes 236–37 and accompanying text (describing Virginia's narrow opt-out right), *and supra* note 267 and accompanying text (describing Colorado's narrow opt-out right).

269. *See supra* note 266 and accompanying text.

270. *See supra* notes 194–98 and accompanying text.

271. *See, e.g.*, COLO. REV. STAT. § 6-1-1311(1)(b) (2021) (effective July 1, 2023); *id.* § 6-1-1310.

CCPA and BIPA).[272] Instead, like under VCDPA, enforcement falls entirely on the state, but with three key deviations. First, CPA temporarily adopts the cure period limited under CCPA[273] and adopted by VCDPA[274] and extends it to sixty days.[275] Second, CPA vests enforcement authority mainly in the state's attorney general but extends that authority to district attorneys.[276] And third, CPA grants the attorney general limited rulemaking power to clarify obligations under the law.[277]

These legislative choices suggest that, rather than simply expand CCPA or VCDPA on their terms, CPA adopts a new approach to data propertization. CPA, for example, hews close to VCDPA by adopting a safe harbor provision in the short run but also provides for the repeal of that provision in the long run.[278] Also, although CPA does not establish an agency tasked with enforcing the law, CPA nonetheless extends the right of action beyond the attorney general to district attorneys[279] and grants the attorney general limited rulemaking power to preempt potentially weak court interpretations of the law with fully informed, prospective interpretations.[280]

3. Moving Forward

CPA is not effective until July 1, 2023,[281] but gaps in data propertization are already becoming evident. The coverage between BIPA, CCPA, VCDPA, and CPA already differs, but additional differences in the rights and enforcement mechanisms among the four only serve to further jeopardize the development of a strong, coherent property interest in data. For example, where the strength of an owner's exclusionary right determines the strength of a property interest,[282] Virginians' and Coloradoans' property interest in sensitive data is stronger than Californians' simply because VCDPA and CPA adopt an opt-in approach, whereas CCPA adopts an opt-out approach.[283] Similarly, where a property interest is only as strong as the enforcement mechanisms designed to protect it,[284] more forgiving safe

272. *See supra* notes 200–01 and accompanying text (CCPA); *supra* notes 136–38 (BIPA).
273. The CCPA safe harbor is available only in private enforcement actions. *See supra* note 201 and accompanying text.
274. *See supra* note 248.
275. *See* COLO. REV. STAT. § 6-1-1311(d) (2021) (effective July 1, 2023).
276. *See id.* § 6-1-1311(a).
277. *See id.* § 6-1-1313.
278. CPA abolishes the safe harbor provision on January 1, 2025. *See id.* § 6-1-1311(d).
279. *See id.* § 6-1-1311(a).
280. *See id.* § 6-1-1313.
281. *See* 2021 Colo. Sess. Laws 3445, § 7.
282. *See supra* notes 64–68 and accompanying text.
283. *Compare supra* notes 241–43 and accompanying text (describing VCDPA's opt-in regime), *and supra* note 263 and accompanying text (describing CPA's opt-in regime), *with supra* notes 176, 179 and accompanying text (describing CCPA's opt-out regime).
284. *See supra* notes 74–81 and accompanying text.

harbor provisions in VCDPA[285] and CPA[286] than in CCPA[287] means that businesses could adopt less stringent data-handling procedures vis-à-vis Virginian and Coloradoan residents than with California residents because VCDPA and CPA allow for a greater margin for error. With so many other differentials in the strength of rights granted and enforcement mechanisms established under each law, it becomes clear why property interests in data are difficult to identify and why there is little agreement on whether data propertization is happening at all.[288]

III. DATA PROPERTIZATION AS IT SHOULD BE

In Part I, this Note discussed how a property interest in data might arise and operate before exploring the scholarship surrounding data propertization. Notwithstanding the ongoing debate, Part II illustrated that data propertization is already underway in Illinois, California, Virginia, and Colorado under the banner of data protection and privacy. Specifically, BIPA, CCPA, VCDPA, and CPA establish property interests in data because they establish rights that mirror the rights of possession, exclusion, and alienability that are emblematic of a property interest.[289]

Yet, Part II also illustrated that gaps and differences among the quartet jeopardize the development of a strong, coherent property interest. To address this issue, this Note prescribes a harmonized bundle of rights best suited to developing property interests in data and argues that those rights should be codified in federal law, dually enforced through agency enforcement and a private right of action. Such an approach would eliminate gaps between existing data propertization laws and stop the proliferation of others as more states seek to enact similar laws.[290]

---

285. *See supra* note 248 and accompanying text.

286. *See supra* notes 273–75, 278 and accompanying text.

287. The CCPA safe harbor is available only in private enforcement actions. *See supra* note 201 and accompanying text.

288. *See, e.g.*, Determann, *supra* note 98, at 25 ("[E]xcept for exclusion rights, data protection and privacy laws diverge from property laws.").

289. *See supra* Parts II.A (BIPA), II.B (CCPA), II.C (VCDPA), and II.D (CPA).

290. The Indiana Senate notably passed its own version of a data protection and privacy law, S.B. 358, on February 1, 2022. *See Indiana Senate Unanimously Passes Privacy* Bill, IAPP (Feb. 2, 2022), https://iapp.org/news/a/indiana-senate-unanimously-passes-privacy-bill/ [https://perma.cc/65GV-3NA3]. Recent reporting suggests that the bill largely mirrors VCDPA and will likely be enacted into law after it is submitted to the Indiana House of Representatives for a vote. *See* Jake Holland, *Indiana Senate Passes Consumer Privacy Bill Lacking Right to Sue*, BLOOMBERG L. (Feb. 2, 2022, 2:00 PM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X5OK3CM4000000?bna_news_filter=privacy-and-data-security [https://perma.cc/YH96-ET8R]. The bill's swift passage reinforces this Note's prediction of increased fragmentation in approaches to data propertization and its claim that a harmonized federal law is increasingly needed. These considerations are top of mind as Massachusetts, Minnesota, New York, North Carolina, Ohio, and Pennsylvania, among other states, ramp up their efforts to advance similar data protection and privacy legislation. *See* Taylor Kay Lively, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/4C8W-DGQ8] (Jan. 20, 2022).

A. Toward a Harmonization of Data Property Rights

"Roughly six-in-ten Americans (63%) say they have very little or no understanding of the laws and regulations that are currently in place to protect their privacy."[291] This is worrisome considering mounting efforts to empower Americans to take control of their data. Does reform really occur if no one notices it is happening? To establish strong property interests in data, this section argues that federal law must grant clear, consistent, and strong rights to possess, exclude, and alienate in the first instance. Specifically, this Note proposes the following bundle of rights adopted from CCPA, VCDPA, and CPA: the right to possess should mirror existing rights to know and access the same types of data.[292] The right to exclude should mirror existing rights to delete but adopt the Virginian and Coloradoan approach establishing a hybrid right to opt in and out of data collection and use.[293] Lastly, the right to alienate should mirror existing rights to portability but adopt the Californian approach to the right to nondiscrimination, which provides a narrow exception for commodifying data.[294] Harmonization in this fashion will not only unify CCPA, VCDPA, and CPA but will affirm BIPA's embrace of data propertization by expanding its definitional coverage,[295] established rights,[296] and framework for enforcement.[297]

1. The Right to Possession

Of the three rights, it is easiest to establish a harmonized right to possession because CCPA, VCDPA, and CPA already agree on the basics: data protection and privacy laws must cover a broad swath of data[298] and empower consumers with the right to know what data is being collected[299] and the right to access that data.[300] Combining CCPA, VCDPA, and CPA approaches to possessory rights would harmonize data propertization regimes by establishing a singular definition of data.[301] Collapsing BIPA into that regime would additionally provide a considerable harmonizing

291. PEW RSCH. CTR., *supra* note 9, at 10.
292. *See infra* Part III.A.1.
293. *See infra* Part III.A.2.
294. *See infra* Part III.A.3.
295. BIPA only propertizes biometric data, *see supra* note 120, while CCPA, VCDPA, and CPA all cover a larger swath of data. *See supra* notes 159–67 and accompanying text (CCPA); *supra* notes 223–25 and accompanying text (VCDPA), *supra* note 256 and accompanying text (CPA).
296. BIPA does not establish the same bundle of rights that CCPA, VCDPA, and CPA do. *See supra* Part II.A.1.
297. BIPA does not establish agency enforcement of the law. *See supra* Part II.A.2.
298. *See supra* notes 159–67 and accompanying text (CCPA); *supra* notes 223–25 and accompanying text (VCDPA); *supra* note 256 and accompanying text (CPA).
299. *See supra* notes 169–70 and accompanying text (CCPA); *supra* note 226 and accompanying text (VCDPA); *supra* note 259 and accompanying text (CPA).
300. *See supra* note 171 and accompanying text (CCPA); *supra* note 227 and accompanying text (VCDPA); *supra* note 259 and accompanying text (CPA).
301. For their respective definitions of covered data, see CAL. CIV. CODE § 1798.140(o)(1) (West 2021); VA. CODE ANN. § 59.1-575 (2021) (effective Jan. 1, 2023); COLO. REV. STAT. § 6-1-1303(17) (2021) (effective July 1, 2023).

effect, as it would expand the law to cover more types of Illinoisan data beyond biometric data.[302]

2. The Right to Exclude

Next, establishing a harmonized right to exclude is essential to forming a more resolute property interest in data.[303] Under current data propertization regimes, the right to exclude translates into the right to delete data in another's possession[304] and either the right to opt in[305] or out[306] of data collection and use. Establishing a harmonized right to delete in the first instance is key to bolstering the property interest as it recognizes the idea that businesses hold others' data only for as long as the owner wishes. In other words, an individual's exercise of the right to delete signifies a retraction of consent, at which point businesses must end their possession by deleting the data from their servers and records.

Additional duties that bar unilateral subsequent transfers of data,[307] mandate regular security practices,[308] and require data minimization principles[309] also enhance a data owner's property interest by ensuring that those without permission to access their data continue to be excluded from it. Specifically, they address issues arising from data's non-rivalry and non-excludability[310] by establishing legal duties designed to protect the data from exfiltration or theft to the maximum extent possible. Accordingly, incorporating those duties into a harmonized property interest in data would

302. *See supra* note 120.

303. *See supra* notes 64–68 and accompanying text.

304. *See supra* note 175 and accompanying text (CCPA); *supra* note 228 and accompanying text (VCDPA); *supra* note 260 and accompanying text (CPA). In Illinois, the right to exclude under BIPA preempts individual choice and requires the destruction of biometric data once the initial purpose for its collection has been satisfied. *See* 740 ILL. COMP. STAT. 14/15(a) (2021). Such a strong requirement is likely unnecessary for all types of data, and a harmonized right to exclude should instead prioritize an individual's right to affirmatively delete data.

305. BIPA's opt-in right imposes an informed consent requirement for all data covered by the law. *See supra* notes 124–26, 129 and accompanying text. VCDPA and CPA, meanwhile, only impose an informed consent requirement for a narrow set of sensitive data. *See supra* notes 241–43 and accompanying text (VCDPA); *supra* note 263 and accompanying text (CPA).

306. *See supra* note 176 and accompanying text (CCPA); *supra* note 229 and accompanying text (regarding nonsensitive data under VCDPA,); *supra* note 261 and accompanying text (regarding nonsensitive data under CPA).

307. *See supra* notes 127–28 and accompanying text (BIPA); *supra* notes 170, 173 and accompanying text (CCPA).

308. *See supra* notes 131–32 and accompanying text (BIPA); *supra* notes 233–34 and accompanying text (VCDPA).

309. *See supra* note 133 and accompanying text (BIPA); *supra* note 172 and accompanying text (CCPA); *supra* note 232 and accompanying text (VCDPA); *supra* note 264 and accompanying text (CPA).

310. *See supra* notes 42–43 and accompanying text.

limit moral hazard concerns[311] and solidify the idea that businesses and other entities should be responsible custodians of the data in their possession.[312]

Under the right to opt in, individuals hold all the power because every business needs consent before that business can access someone else's data.[313] A right to opt in could implicate all data regulated by the law, as is the case with BIPA,[314] or only a small subset of data meriting additional protection, as is the case with VCDPA[315] and CPA.[316] Alternatively, under a right to opt out under CCPA,[317] VCDPA,[318] and CPA,[319] a consumer may prospectively exclude businesses from thereafter engaging in certain data activities—CCPA would ban all subsequent sale and sharing of that data,[320] whereas VCDPA and CPA would only ban the subsequent sale, the use in targeted advertising, and the use in profiling of that data.[321]

This Note takes the position that the Virginian and Coloradoan approaches to consent,[322] which establish an opt-out regime for most types of data but craft a narrow opt-in regime for sensitive data, is the proper approach. Under this hybrid approach, consent is required to collect or use a narrow set of "sensitive" data but not for a wider set of "regular" data. This balances economic concerns that an opt-in right that applies to all data would result in wasteful and inefficient transaction costs[323] with the reality that some forms of data warrant heightened protection anyway, given the rise in data harms that target such data.[324] Similarly, where an opt-out right places the burden on individuals to monitor and affirmatively assert their property interests in data, a limited opt-in right at least recognizes a heightened privacy interest in sensitive data by displacing a subset of those monitoring costs onto collecting entities. In this regard, CCPA, VCDPA, and CPA provide an adequate baseline for distinguishing between sensitive and regular data:[325] they all protect data that implicate a high privacy interest, such as biometric data and

311. *See supra* note 41 and accompanying text; *supra* note 88.

312. *See supra* notes 69–72 and accompanying text; *see also supra* note 265 and accompanying text (citing prefatory language in CPA supporting the existence of such a duty).

313. *See supra* notes 85, 129.

314. *See supra* notes 126, 129 and accompanying text.

315. *See supra* notes 241–43 and accompanying text.

316. *See supra* note 263 and accompanying text.

317. *See supra* note 176 and accompanying text

318. *See supra* note 229 and accompanying text.

319. *See supra* note 261 and accompanying text.

320. *See supra* note 176 and accompanying text.

321. *See supra* note 236 and accompanying text (VCDPA); *supra* note 267 and accompanying text (CPA).

322. *See supra* notes 241–43 and accompanying text (VCDPA); *supra* note 263 and accompanying text (CPA).

323. *See supra* notes 98–101.

324. *See, e.g.*, *supra* notes 9–12 and accompanying text; *see also supra* notes 65–67 and accompanying text (arguing that the strength of a property protection afforded must reflect the privacy interest at stake).

325. For their respective definitions of "sensitive data," see CAL. CIV. CODE § 1798.140(ae) (West 2021) (effective Jan. 1, 2023); VA. CODE ANN. § 59.1-575 (2021) (effective Jan. 1, 2023); COLO. REV. STAT. § 6-1-1303(24) (2021) (effective July 1, 2023).

personal data revealing sex life or sexual orientation.[326] The exact delineation under a harmonized regime should be hammered out by regulation so that the property interests can remain flexible and shift over time as needed.[327]

Lastly, because exclusionary rights are central to any property interest,[328] the exclusion must be strong: any use, sale, and sharing of data must be prohibited before individuals exercise their opt-in right and after they exercise their opt-out right.[329] This Note already circumscribes the opt-in right within a narrow class of sensitive data such that a harmonized approach would minimize the number of times businesses will need consent to collect or use that data. And there is very little justification for limiting the opt-out right—if most consumers are ignorant of or do not care about how their data is being exchanged or monetized,[330] it follows that only the few who care most about their data will take the steps to affirmatively exercise that right anyway.[331]

3. The Right to Alienate

Lastly, this Note takes the position that a harmonized right to alienate should prioritize data protection over data commodification to address concerns that commodification may entrench existing inequalities through consumer exploitation.[332] Accordingly, rather than promoting alienation through institutions that encourage individuals to sell their data,[333] an effective data propertization regime would passively protect alienation decisions as they are made.

This is achieved by enshrining a right to nondiscrimination[334] and a right to portability.[335] By prohibiting businesses from retaliating when data owners exercise their rights and actively requiring businesses to help data owners move their data as they wish, these rights protect an individual's alienation decisions rather than encourage them. This is not to say, however, that all commodification should be prohibited. The nondiscrimination right should include a narrow exception allowing businesses to offer a different

326. *See supra* note 325.
327. *See infra* note 370 and accompanying text.
328. *See supra* notes 64–68 and accompanying text.
329. Only CCPA bars the subsequent sale *and* sharing of data. VCDPA and CPA only bar data's subsequent sale, use in targeted advertising, and use in profiling. *See supra* notes 320–21 and accompanying text.
330. *See supra* notes 102–05 and accompanying text.
331. *See supra* note 85.
332. *See supra* note 106 and accompanying text.
333. *See, e.g.*, Laudon, *supra* note 25, at 99–101 (proposing the establishment of a "National Information Market"); Lanier & Weyl, *supra* note 25 (proposing the establishment of organizations called "mediators of individual data" charged with negotiating data royalties and wages on behalf of data owners).
334. *See supra* notes 185–86 and accompanying text (CCPA); *supra* note 231 and accompanying text (VCDPA). Illinois and Colorado do not establish a right to nondiscrimination. *See supra* Parts II.A.1, II.D.1.
335. *See supra* note 184 and accompanying text (CCPA); *supra* note 230 and accompanying text (VCDPA); *supra* note 262 and accompanying text (CPA).

price or quality of goods depending on the value of data excluded from them.[336] This narrow exception serves the important end of balancing the criticisms that consumers may be ignorant of or do not care about how their data is being exchanged and monetized[337] with the reality that data can sometimes serve as a proxy for money in transactions for services.[338] More importantly, this exception serves an information-forcing purpose that leads to increased innovation: if businesses want to continue receiving consumer data through nonmonetary means, they will need to better explain how, why, and to what extent they are providing services in exchange for data while providing a high enough quality of service to convince consumers either to opt in to the collection of sensitive data or to abstain from exercising their right to opt out of regular data collection.[339]

B. Toward a Federalized Property Interest in Data

By selectively adopting the most effective features of current data propertization laws, a harmonized bundle of data rights to possess, exclude, and alienate bolster the underlying property interest in data. In this section, this Note examines justifications for codifying such a property interest in federal law and justifications for enforcing the underlying rights and correlative duties through an administrative agency.

1. Establishing Federal Data Property Rights

Federal data laws in the United States are uncoordinated: some health data is protected under the Health Insurance Portability and Accounting Act of 1996,[340] credit data is protected under the Fair Credit Reporting Act,[341] financial data is protected by the Gramm-Leach-Bliley Act,[342] and so on.[343] This fragmentation leads to two undesired results: it scatters what may otherwise be a coherent set of rights and duties across the U.S. Code and encourages states to fill resulting gaps in privacy law, which only adds further to fragmentation of the nascent property interest.

Worse yet, the state problem is a compounding one. For example, scholars have already begun to address mounting concerns that federal law may

336. This is already the approach under CCPA's Spotify exception. *See supra* note 186.

337. *See supra* note 105 and accompanying text.

338. *See supra* notes 103–04 and accompanying text.

339. *See* Schwartz, *supra* note 94, at 2100 ("[Information-forcing] . . . would place pressure on the better-informed party to disclose material information about how personal data will be used.").

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

341. Pub. L. No. 90-321, 82 Stat. 146 (1968) (codified as amended in scattered sections of 15 and 18 U.S.C.).

342. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12, 15, and 18 U.S.C.).

343. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/Q9LG-N8T3].

preempt current data propertization laws.[344] More importantly, permutations in state-prescribed definitions, rights, and enforcement mechanisms build on each other to aggrandize gaps between data propertization regimes. For example, where gaps in coverage prevent Illinoisans from asserting property rights to nonbiometric data in the same way that Californians, Virginians, and Coloradoans can,[345] the lack of a right to nondiscrimination prevents Illinoisans and Coloradoans from exchanging their data for valuable services in a way that Californians and Virginians are able to.[346] All this, as the utter lack of a private right of action under VCDPA and CPA bars Virginian and Coloradoan data owners from directly asserting their property rights, while its availability under BIPA and CCPA empowers Illinoisans and Californians to do so.[347]

These and other gaps not only impose unnecessarily variable compliance costs and establish inefficient barriers to entry[348] but also increase the risk that individuals will have starkly different conceptions of what they can and cannot do with their data.[349] Because data is an intangible good[350] that does not know borders,[351] adopting a state-dependent approach to data propertization necessarily means that each law will always be weaker in some respects and stronger in others than the rest. Moreover, as GDPR did not propertize data on standard terms worldwide through an unstoppable Brussels Effect,[352] no single state law can ever do the same for the United

344. *See generally, e.g.*, Katherine Q. Morrow, *Preemption Problem: Does ERISA Preempt the California Consumer Privacy Act?*, 99 N.C. L. REV. 789 (2021) (addressing conflicts with the Employee Retirement Income Security Act); Lauren Davis, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. BANKING INST. 499 (2020) (addressing conflict with the Gramm-Leach-Bliley Act). *Compare, e.g.*, Kiran K. Jeevanjee, Comment, *Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California's CCPA from Setting National Privacy Law*, 70 AM. U. L. REV. F. 75 (2020) (arguing that CCPA likely cannot withstand a constitutional challenge on Commerce Clause grounds), *with* Russell Spivak, *Too Big a Fish in the Digital Pond?: The California Consumer Privacy Act and the Dormant Commerce Clause*, 88 U. CIN. L. REV. 475 (2019) (arguing the opposite).

345. *See supra* note 295.

346. *See supra* note 186.

347. *Compare supra* notes 246–50 and accompanying text (VCDPA), *and supra* note 271 and accompanying text (CPA), *with supra* notes 136–47 and accompanying text (BIPA), *and supra* notes 200–03 and accompanying text (CCPA).

348. For example, a report on CCPA's impact suggests that California businesses "will be at a disadvantage when competing in markets outside of California, as they will be faced with higher compliance costs relative to their competitors," but will also gain a competitive advantage through "barriers to entry for future competitors considering entering into the California market." BERKELEY ECON. ADVISING & RSCH., *supra* note 206, at 31–32.

349. *See* Simon G. Davies, *Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 147 (Philip E. Agre & Marc Rotenberg eds., 1997) ("The citizens of Western industrialized countries want privacy, but feel it is extinct. They are aware of the loss of privacy, but feel powerless to defend themselves against intrusive practices. These feelings may be due in part to the increasing difficulty of defining privacy rights.").

350. *See supra* note 42 and accompanying text.

351. *See supra* notes 39–41 and accompanying text.

352. *See supra* notes 115–17 and accompanying text.

States.[353] Only a federalized data propertization regime that codifies harmonized rights to possess, exclude, and alienate data within federal law would fix these issues.

2. Protecting Federal Data Property Rights

Of course, part of establishing a federal property interest in data is enforcing the rights and duties that come with it.[354] In this regard, federal enforcement of the interest can correct power imbalances in which data owners with diffuse interests would be otherwise disadvantaged when facing organized data collectors with more focused interests.[355] Additionally, instrumentalization of federal agencies will help to ensure that property interests in data are adequately monitored and protected where an individual's personal data may not have a high enough value to justify private action.[356] Accordingly, enforcement of a property interest in data must occur by explicitly expanding the authority of the Federal Trade Commission (FTC) to investigate and litigate data harms[357] or by establishing a new, separate agency to do the same.[358] In this regard, the Californian approach in establishing a new agency to enforce CCPA[359] is an appropriate one. Note, however, that in protecting property interests in data, federal authorities must take special care to find an optimal level of enforcement that neither merely consists of burying companies in compliance obligations[360] or imposing

353. Colorado and Virginia enacted their data propertization laws despite the California Effect, and California enacted CCPA despite the Brussels and Illinois Effects. *See supra* notes 115–17 and accompanying text (discussing the Brussels Effect); *supra* notes 148–52 and accompanying text (discussing the Illinois Effect); *supra* notes 211–12 and accompanying text (discussing the California Effect).

354. *See supra* notes 74–81 and accompanying text.

355. Under public choice theory, "large collectivities with diffuse interests will be systematically disadvantaged in the political process as compared to smaller groups with more acute interests because larger groups face higher organizing costs and are affected more severely by incentives to free ride." Amy Kapczynski, *The Access to Knowledge Mobilization and the New Politics of Intellectual Property*, 117 YALE L.J. 804, 811 (2008).

356. *See* Schwartz, *supra* note 94, at 2108–09.

357. The FTC currently asserts jurisdiction over data harm investigations and litigation by claiming that the harms were the result of unfair and deceptive trade practices. *See* FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 1 (2021). This is an unnecessarily circuitous route. Expanding the FTC's regulatory authority to explicitly cover data harms would streamline and bolster those actions while avoiding the costs of establishing an entirely new agency tasked with doing the same.

358. *See, e.g.*, Kirsten Gillibrand, *Facebook and Social Media Endanger Americans. We Need a Federal Data Agency*, NBC THINK (Oct. 25, 2021, 11:55 AM), https://www.nbcnews.com/think/politics-policy/facebook-rcna3704 [https://perma.cc/RA7E-VLZ7] (proposing a separate agency charged with monitoring data harms).

359. *See supra* notes 194–98 and accompanying text.

360. *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 834 (2020) (arguing that "when . . . merely symbolic structures proliferate, they undermine the substantive power of the law and shift the discourse of power, all to the detriment of consumer privacy").

slaps on the wrist[361] nor results in a disproportionately large burden on small businesses.[362]

A federal agency tasked with protecting property interests in data also requires significant regulatory authority.[363] Here, the controlling agency should be structured like the California Privacy Protection Agency, which is run by members with relevant expertise[364] empowered to enforce CCPA and promulgate regulations interpreting it.[365] At the federal level, such authority would arise from the Administrative Procedure Act (APA),[366] which would allow for substantial deference to agency expertise when reviewing decisions of policy or interpretations of relevant data propertization legislation.[367] Considering the rapidly changing nature of technology,[368] this flexibility will provide the agency with a margin for maneuver so that the agency can respond adequately and swiftly to new data issues as they arise. Notice-and-comment rulemaking under the APA,[369] for example, will allow the agency to adjust the opt-in regime by reforming the line between sensitive and nonsensitive data as the privacy interest in different types of data shifts over time.[370]

Last in the issue of enforcement is the question of a private right of action. Admittedly, more research is needed on whether and how much private enforcement can and should be allowed under federal law. As we saw, BIPA allows private actions to survive without an injury in fact.[371] Under federal law, however, actions must present a "concrete *and* particularized" injury in

361. *See* Emily Stewart, *A $5 Billion Fine Won't Fix Facebook. Here's What Would.*, VOX (Sept. 10, 2019, 7:30 AM), https://www.vox.com/business-and-finance/2019/9/10/20857109/facebook-equifax-companies-break-law [https://perma.cc/ZK26-N38N] ("If a monetary penalty is big enough to affect the company's bottom line or change the way it does business, it can be effective. But in many cases, it's not, especially when it comes to multi-billion-dollar corporations. And fines ultimately get passed onto shareholders and workers, not company decision makers.").

362. *See, e.g.*, BERKELEY ECON. ADVISING & RSCH., *supra* note 206, at 31 ("Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.").

363. Both CCPA and CPA provide some form of regulatory and rulemaking authority to various agencies and executive offices. *See supra* notes 194–96 and accompanying text (CCPA); *supra* note 277 and accompanying text (CPA).

364. *See supra* note 198 and accompanying text; *see also* CAL. CIV. CODE § 1798.199.15 (West 2021) (outlining qualifications and conduct expected of board members).

365. *See* CAL. CIV. CODE § 1798.199.40(b) (West 2021).

366. 5 U.S.C. §§ 500–596.

367. Under APA's review scheme, 5 U.S.C. § 706, policy decisions are reviewed under an "arbitrary and capricious" standard. Motor Vehicles Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 34 (1983). Decisions rooted in interpretations of an underlying federal statute are reviewed under a reasonableness standard. *See* Chevron U.S.A., Inc. v. Nat'l Res. Def. Council, 467 U.S. 837, 844–45 (1984).

368. *See supra* note 7 and accompanying text.

369. *See* 5 U.S.C. § 553.

370. *See supra* notes 322–27 and accompanying text; *see also* Schwartz, *supra* note 94, at 2098–99 ("To ensure that the opt-in default leads to meaningful disclosure of additional information, . . . the government must have a significant role in regulating the way that notice of privacy practices is provided.").

371. *See supra* notes 145–47 and accompanying text.

fact to satisfy standing requirements in federal court.[372] As a result, even if federal data propertization legislation granted a private right of action for litigation of injuries in law, standing requirements might keep such lawsuits from entering federal courthouse doors.[373] At the very least, there should be some form of private enforcement because leaving enforcement solely in the hands of the state would leave data owners without viable methods for privately obtaining compensation for data harms or asserting moral rights to their property.[374]

This Note does not seek to ignore the risk of opportunism[375] and the concern that the cost of private litigation may not justify its benefits.[376] Instead, it argues that some form of private enforcement is needed to supplement (rather than supplant) administrative enforcement.[377] Accordingly, a proper approach to enforcement would hew toward the Illinoisan[378] and Californian regimes,[379] which allow some form of private enforcement, unlike the Virginian[380] and Coloradoan[381] approaches, which leave enforcement completely in the hands of state attorneys general. An effective federalized property interest in data would establish not only a robust set of rights but also a strong set of enforcement mechanisms designed to protect them.

CONCLUSION

Data propertization is underway, and there is no stopping it. This Note began by examining data propertization through the lens of data and property. Then, by analyzing state laws that fly under the banner of data protection and privacy, this Note illustrated that carefully crafted rights, duties, and enforcement mechanisms have begun to push data legislation away from traditional consumer protection and toward data propertization. Methods range in their embrace of property from those that prioritize exclusivity[382] to those that build regimes around a bundle of rights,[383] but this Note asserted that the ideal approach to empowering consumers and preventing data harms hews toward the latter. Through a robust regime of rights, duties, and

372. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016); *see also* Transunion LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021); U.S. CONST. art. III, § 2.

373. *See supra* note 209.

374. *See supra* notes 75–80 and accompanying text.

375. *See supra* note 247 and accompanying text.

376. *See supra* note 356 and accompanying text.

377. *See supra* notes 75–80 and accompanying text (noting that both avenues for enforcement serve distinct yet complementary goals).

378. *See supra* notes 136–47 and accompanying text.

379. *See supra* note 200 and accompanying text.

380. *See supra* notes 246–47 and accompanying text.

381. *See supra* note 276 and accompanying text.

382. *See* Own Your Own Data Act, S. 806, 116th Cong. (2019).

383. *See, e.g.*, Data Protection Act of 2020, S. 3300, 116th Cong. (2020); 740 ILL. COMP. STAT. 14/1–99 (2021); CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2021); VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2021) (effective Jan. 1, 2023); COLO. REV. STAT. §§ 6-1-1301 to 6-1-1313 (2021) (effective July 1, 2023).

enforcement mechanisms, property law can grant ownership of data and protect it in one fell swoop.

Though this approach to data propertization has shown some success in Illinois, California, Virginia, and Colorado to the point of limited regulatory globalization, a state-led approach risks becoming too fragmented to be effective. Because data knows no borders, border-conscious variations between the quartet of existing data propertization laws threaten to disrupt the data propertization narrative and risk creating more problems than it purports to solve. Accordingly, the federal data propertization regime proposed by this Note has the greatest potential to establish a more cohesive and more significant property interest in data that is more capable of withstanding a new age of digital harms.