BEYOND DATA OWNERSHIP

Ignacio Cofone†

Proposals for data ownership are widely misunderstood, aim at the wrong goal, and would be self-defeating if implemented. This Article, first, shows that data ownership proposals do not argue for the bundle of ownership rights that exists over property at common law. Instead, these proposals focus on transferring rights over personal information solely through consent.

Second, this Article shows the flaws of a property approach to personal information. Such an approach magnifies well-known problems of consent in privacy law: asymmetric information, asymmetric bargaining power, and leaving out inferred data. It also creates a fatal problem: moral hazard where corporations lack incentives to mitigate privacy harm. The moral hazard problem makes data ownership self-defeating. Recognizing these deficiencies entails abandoning the idea that property over personal data can achieve meaningful protection.

This Article, third, develops proposals for privacy law reform amidst a national debate on how to formulate federal and state privacy statutes. It argues for a combination of what Calabresi and Melamed call property and liability rules. A mixed rule system is essential because property rules alone fail to protect data

† Assistant Professor and Canada Research Chair in A.I. Law & Data Governance, McGill University Faculty of Law, ignacio.cofone@mcgill.ca. Many thanks to BJ Ard, Lisa Austin, Michael Beauvais, Elettra Bietti, Johannes Buchheim, Rebecca Crootof, Christopher Essert, Inge Graef, Nikolas Guggenberger, Tom Haley, Claudia Haupt, Chris Howard, Martin Husovec, Shaz Jameson, Robert Leckey, Anthony Niblett, Przemyslaw Palka, Adriana Robertson, Teresa Scassa, Alicia Solow-Niederman, Mark Verstraete, Jacob Victor, Salome Viljoen, and Ari Waldman for their helpful comments. This Article also benefited from presentations at the Council of Europe Convention 108, Tilburg University TILTing Perspectives 2021 Conference, Torcuato Di Tella Regulation Workshop, University of Toronto Law & Economics Workshop, and Yale Law School. I gratefully acknowledge that financial support for research assistance was provided by the Social Sciences and Humanities Research Council (Insight Development Grant) and the Canada Research Chairs Program; that an academic visit at the Tilburg Institute for Law, Technology, & Society to work on this project was supported by Microsoft; and that this Article received the Council of Europe Stefano Rodota Award Special Jury Mention. I also thank Ana Qarri, Jeremy Wiener, Vanessa Di Feo, and Martina Kneifel for their fantastic research assistance and the editors of the *Cardozo Law Review* for their help during the editing process.

subjects from future uses and abuses of their personal information. This Article implements this idea with two recommendations. First, it proposes bolstering private rights of action for privacy harm unattached to statutory breach. Second, it proposes reinforcing ongoing use restrictions over personal data by strengthening the purpose limitation principle, an underutilized ongoing use restriction in American law.

TABLE OF CONTENTS

INTRODUCTION

Is data ownership a viable way of protecting privacy? The idea that privacy should entail ownership over one's personal information has gained popularity in legislative proposals,[1] the media,[2] and academic circles.[3] While a broad version of this idea is not new, novel permutations have appeared, for example, in pay-for-privacy,[4] data as labor,[5] and blockchain.[6]

---

1 *See, e.g.*, Own Your Own Data Act, S. 806, 116th Cong. (as introduced by Sen. John Kennedy, Mar. 14, 2019); *see also* Angel Au-Yeung, *California Wants to Copy Alaska and Pay People a "Data Dividend." Is It Realistic?*, FORBES (Feb. 14, 2019, 10:04 AM), https://www.forbes.com/sites/angelauyeung/2019/02/14/california-wants-to-copy-alaska-and-pay-people-a-data-dividend—is-it-realistic/?sh=61e758521358 [https://perma.cc/72DE-ZYWK].

2 *See infra* Section I.A.

3 *See infra* Section I.B.

4 Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1400–28 (2017) (showing that pay for privacy models turn privacy into a tradeable product).

5 ERIC A. POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY 209–33 (2018) (including in the proposal both personal and non-personal information).

6 Ben Dickson, *How Blockchain Solves the Complicated Data-Ownership Problem*, NEXT WEB (Aug. 17, 2017), https://thenextweb.com/news/blockchain-solves-complicated-data-ownership-problem [https://perma.cc/X4TF-YJJ3] ("Blockchain technology provides an alternative that gives the ownership of data back to users.").

This Article engages with data ownership in three ways. First, it revisits and improves popular understandings of data ownership proposals. Second, it identifies a problem that makes data ownership self-defeating. Third, based on that critique, it develops proposals for privacy law reform.

Data ownership proposals contain a conceptual ambiguity. Despite the language that proponents use,[7] they have not proposed creating ownership rights over data. Ownership rights (i.e., property rights) constitute closed-form in rem rights. But data ownership proposals do not advocate for implementing this type of right over personal data.

Instead, these proposals advocate for reinforcing consent and creating a marketplace for data that aims to maximize data-subject control over their personal information. Such a market is supposed to extract larger ex-ante compensation for users. The proposals rely not on property *rights* but on Calabresi-Melamed property *rules*, which are consequentially different. Property rules stipulate that a right can only be transferred with consent.[8] Arguing that rights over personal data should be given away solely by consent refers to property rules—even if some proponents may believe themselves to be applying property rights. One can see this from the language used in the proposals, the absence of ownership rights' key elements, and the emphasis proponents place on consent, bargaining, and compensation.

In other words, data ownership is usually seen as *the view that people should have an ownership right over data*. But it is better understood as *the view that people should have a right over their data (whatever kind of right it is) protected solely by property rules*.[9] In clarifying this conceptual ambiguity, this Article refers to these proposals as "data property."

This clarification shows that data property is subject to criticism on new grounds. Prior scholarship has shown that data property is undesirable because it leaves out important values and dimensions of privacy.[10] Understanding that data property proposals defend transfer rules—not ownership—also exposes two sets of problems that have so far not been identified: consent problems and moral hazard.

---

7 *See infra* Part I.

8 Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1089–93 (1972).

9 *See infra* Section II.B.

10 *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1408–16 (2000); *see also infra* Section II.C.

First, data property relies on—and would magnify the role of—consent in privacy.[11] Such reliance on consent, which Daniel Solove refers to as "privacy self-management,"[12] has been criticized as fundamentally flawed. Seeing how data property relies on consent makes clear that it inevitably inherits and magnifies consent's deficiencies: asymmetric information,[13] unequal bargaining power,[14] and data aggregation.[15] Due to these problems, even if data property may seem like it would provide strong protection, it cannot improve data subjects' vulnerable situation.

Second, understanding data property as transfer rules allows one to see how data property is counterproductive when it comes to achieving its own aim: promoting consumer control. Relying solely on property rules would lead to inadequate and insufficient control because it would eliminate incentives for companies to take efficient levels of care after a data transaction. Therefore, they generate a moral hazard: by not facing the consequences of the losses they produce, companies would have larger incentives to engage in risky uses and disclosures of personal data. This would further reduce people's long-term control over their personal data and expose them to more harm. This moral hazard makes data property self-defeating.[16]

This critique informs normative debates in privacy law that do not resort to the language of property but nevertheless share some of data property's elements by relying on consent. The failures of data property show that ex-post accountability is a necessary condition for robust privacy protection. Privacy law must protect privacy rights with both consent-based rules (which operate ex-ante) and accountability mechanisms (which operate ex-post). Statutory privacy seems to lean too heavily on the side of the former. This Article proposes two ways to address this: (i) combining consent requirements with new private rights of action and (ii) keeping and reinforcing restrictions on the use of personal data.

---

11 *See* Václav Janeček, *Ownership of Personal Data in the Internet of Things*, 34 COMPUT. L. & SEC. REV. 1039, 1041 (2018); *see also infra* Part II.

12 Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882–83 (2013); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 444 (2016) (explaining the narrative of privacy self-management).

13 *See* Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 130–52, 165–72; *see also infra* Section III.A.

14 *See infra* Section III.B.

15 *See infra* Section III.C.

16 *See infra* Part IV.

The first proposal involves establishing private rights of action to enforce privacy.[17] Liability responds to the market reality by (i) not relying on unequal bargaining between consumers and companies and (ii) encompassing inferred data. Liability addresses the moral hazard problem by forcing companies to internalize the expected cost of their data use and sharing. Because of these functions, liability can address property rules' deficiencies in protecting privacy.

The second proposal concerns the importance of reinforcing the controversial purpose limitation principle.[18] The purpose limitation principle establishes that personal information must be collected for a specific use and cannot later be given different uses. It is thus the most important ongoing use restriction in statutory privacy. The principle is drawn from the Fair Information Practices Principles, which form the backbone of statutory privacy in the United States.[19] But existing and proposed state laws are divided as to whether to incorporate purpose limitation, and it remains unclear whether an eventual federal privacy statute would.

These proposals are particularly relevant now, as states continue to formulate privacy statutes and the federal government considers a (possibly preemptive) federal privacy statute.[20] Virginia's Consumer Data Protection Act (CDPA) and the Colorado Privacy Act, for example, include purpose limitation but not private rights of action,[21] while the Nevada Privacy of Information Collected on the Internet from Consumers Act (PICICA) includes neither.[22] This Article's proposals can also be implemented while enforcing these statutes. The usefulness of liability can inform courts when ruling on standing for privacy harms recognized by statute, or when determining whether a statute preempts privacy torts. The proposal over purpose limitation can be used by

---

17 *See infra* Part V.

18 *See infra* Part VI.

19 Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 99–112 (2020).

20 Thomas Germain, *State Privacy Laws Move Forward, but Are They Strong Enough?*, CONSUMER REPS. (Feb. 23, 2021), https://www.consumerreports.org/privacy/state-privacy-laws-move-forward [https://perma.cc/5DSN-QD8E]; Jennifer Bryant, *2021 "Best Chance" for US Privacy Legislation*, IAPP (Dec. 7, 2020), https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation [https://perma.cc/4HN5-ERWB] (arguing that a federal privacy statute has never been as likely as it is this legislative year); James Coker, *Will the US Move to a Federal Privacy Law in 2021?*, INFOSECURITY (Dec. 18, 2020), https://www.infosecurity-magazine.com/news/us-move-federal-privacy-law-2021 [https://perma.cc/7KZN-HEPU] (discussing the possibility of a federal privacy statute).

21 H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. § 59.1-571(1)–(2)); COLO. REV. STAT. §§ 6-1-1308, 6-1-1310(1).

22 NEV. REV. STAT. ANN. §§ 603A.320, 603A.360 (LexisNexis 2017); *see also* H.B. 1602, 58th Leg., 1st Sess. (Okla. 2021).

courts or enforcement authorities (state attorneys general and the Federal Trade Commission (FTC)) in interpreting the scope of purpose limitation and, in particular, when assessing whether specified purposes are narrow enough.

This Article proceeds as follows. Part I provides an overview of data property proposals in legislation, the media, private industry, and academia. Part II shows that most of these proposals refer to property rules, not rights, and thus their key element is about trade (not bundles of rights). Part III outlines how existing criticisms of privacy law apply to data property once interpreted correctly. Part IV explains why data property would introduce an additional, fatal flaw that would lead it to defeat itself: moral hazard. Parts V and VI propose two directions to move past the ameliorated version of the moral hazard problem that exists in privacy law. Part V explains how privacy statutes can complement their property rules with liability rules by creating harm-dependent private rights of action. Part VI suggests reinforcing the purpose limitation principle to better ex-post accountability.

I. THE POPULARITY OF DATA PROPERTY

Data property proposals are increasingly popular. Some of them use the language of ownership with phrases like "you should own your data." Some use the language of property rights. Others say people should receive monetary compensation when relinquishing their personal information. These proposals are burgeoning in legislation, public policy, general audience outlets, private industry lobbying, and academia.

A. *Politics, Media, and the Private Industry*

Several proposals in politics, the media, and academia have suggested ownership or property rights over data as a means of increasing data subjects' control over their personal information and, more generally, their privacy.

Legislation is a good example of this trend. For example, the 2019 Own Your Own Data Act attempted to provide people with property rights over their data, developing a licensing system that focused on portability.[23] California has discussed the idea of "data dividends" that

[23] Own Your Own Data Act, S. 806, 116th Cong. (as introduced by Sen. John Kennedy, Mar. 14, 2019).

rely on property over data.[24] Former presidential candidate Andrew Yang has been explicit in his proposal that personal data should be treated as property, meaning that individuals should have ownership over their data.[25] Yang claims that, because individuals are not being paid or not otherwise obtaining value for their data, this denies them autonomy and produces a lack of data dignity.[26] Yang also started a non-profit organization that advocates for treating personal "data as property."[27]

European and Canadian politics have also seen versions of this idea. The Canadian government Committee on Access to Information, Privacy, and Ethics has recommended establishing rules and guidelines regarding data ownership and data sovereignty with the objective of ending the non-consented collection and use of citizens' personal information.[28] More hesitantly, the European Commission launched a consultation group assessing data ownership,[29] and former German Chancellor Angela Merkel argued in favor of a uniform E.U. regulation establishing data ownership.[30]

---

24 Jill Cowan, *How Much Is Your Data Worth?*, N.Y. TIMES (Mar. 25, 2019), https://www.nytimes.com/2019/03/25/us/newsom-hertzberg-data-dividend.html [https://perma.cc/YX8E-T788] (describing California's Governor's proposal).

25 Marty Swant, *Andrew Yang Proposes Digital Data Should Be Treated like a Property Right*, FORBES (Oct. 1, 2019, 4:27 PM), https://www.forbes.com/sites/martyswant/2019/10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/?sh=49c5d6163ab7 [https://perma.cc/62ZH-2UVW].

26 *Regulating Technology Firms in the 21st Century*, YANG2020 (Nov. 14, 2019) [hereinafter *Regulating Technology Firms*], https://2020.yang2020.com/blog/regulating-technology-firms-in-the-21st-century [https://perma.cc/T57L-VHSP]; *see also* NBC News Now, *Andrew Yang Explains Why Digital Data Is Personal Property*, YOUTUBE (Oct. 15, 2019), https://www.youtube.com/watch?v=tSOf0Eh-4dU (last visited Nov. 18, 2021); 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/X7K8-AXP9] (presenting the idea of "data dignity" and arguing that data is a form of labor and taking it without compensation is labor exploitation).

27 Tyler Sonnemaker, *Andrew Yang Wants You to Make Money off Your Data by Making It Your Personal Property*, INSIDER (Nov. 14, 2019, 4:15 PM), https://www.businessinsider.com/andrew-yang-data-ownership-property-right-policy-2019-11 [https://perma.cc/BE8K-K6H5]; Matt Stevens, *Andrew Yang's next Move: A New Nonprofit Organization*, N.Y. TIMES (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/us/politics/andrew-yang-humanity-first.html [https://perma.cc/H7W3-LJDS] (discussing the organization's involvement in property rights over data).

28 BOB ZIMMER, ADDRESSING DIGITAL PRIVACY VULNERABILITIES AND POTENTIAL THREATS TO CANADA'S DEMOCRATIC ELECTORAL PROCESS 23 (2018).

29 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Thriving Data-Driven Economy*, COM (2014) 0442 final (Feb. 7, 2014).

30 *See* Press Release, Merkel: Regulate Ownership of Data (Mar. 18, 2017), https://www.bundesregierung.de/breg-de/aktuelles/merkel-eigentum-an-daten-regeln-745810 [https://perma.cc/A8M7-QBK4].

Similar proposals exist in the media. The Financial Times, for example, argued in 2018 that consumers should be given ownership rights over their personal data.[31] The Economist claimed in 2019 that people must own their personal data as a matter of human rights, stating that "data itself should be treated like property and people should be fairly compensated for it."[32] An article in Forbes argued in 2020 that "it's time to own your data."[33]

This idea is not foreign to the private industry either. Robert Shapiro and Siddhartha Aneja, for example, propose that the government and major companies recognize that people have property rights over their personal information.[34] Customer data platform Segment is explicit in stating that people should own their data.[35] Bird & Bird also developed a whitepaper exploring ownership over data, stating that "new non-exclusive ownership right in data should be created to respond to the EU data economy's demands."[36] Members of the blockchain community have developed similar proposals, with the idea that blockchain can provide people with ownership over data.[37]

---

31 *Data Privacy Rights Require Data Ownership*, FIN. TIMES (Mar. 21, 2018), https://www.ft.com/content/a00ecf9e-2d03-11e8-a34a-7e7563b0b0f4 [https://perma.cc/8E8C-XJRT].

32 Will.I.Am, *We Need to Own Our Data as a Human Right—And Be Compensated for It*, ECONOMIST (Jan. 21, 2019), https://www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it [https://perma.cc/7AGH-CXWD].

33 Dan Demers, *From Complexity to Control: It's Time to Own Your Data*, FORBES (Feb. 27, 2020, 7:45 AM), https://www.forbes.com/sites/forbestechcouncil/2020/02/27/from-complexity-to-control-its-time-to-own-your-data/?sh=42199876ceda [https://perma.cc/PB36-P8Q2] (capitalization alterations omitted).

34 ROBERT SHAPIRO & SIDDHARTHA ANEJA, WHO OWNS AMERICANS' PERSONAL INFORMATION AND WHAT IS IT WORTH? 5 (2019).

35 *Why You Should Own Your Data*, SEGMENT, https://segment.com/academy/intro/why-you-should-own-your-data [https://perma.cc/N9FN-3PL5].

36 BENOIT VAN ASBROECK, JULIEN DEBUSSCHE & JASMIEN CÉSAR, BUILDING THE EUROPEAN DATA ECONOMY 121 (2017) (adding that exclusive ownership would be meaningless in the context of GDPR).

37 *See, e.g.*, David Floyd, *Blockchain Could Make You—Not Equifax—The Owner of Your Data*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/news/blockchain-could-make-you-owner-data-privacy-selling-purchase-history [https://perma.cc/MZ4R-HA93] ("Users of digital services are treated a bit like oblivious gulls who happen to excrete an immensely productive resource, rather than owners of an asset they create. Blockchain technology and related cryptographic techniques could change that, giving us control over our personal data and enabling us to sell it to whomever we please."); Dickson, *supra* note 6 ("Blockchain technology provides an alternative that gives the ownership of data back to users."); Ben Dickson, *What's the Value of Blockchain to Consumers?*, TECHTALKS (June 1, 2017), https://bdtechtalks.com/2017/06/01/whats-the-value-of-blockchain-to-consumers [https://perma.cc/TX5H-2K36] ("So what is the tangible value of blockchain to consumers? I believe it's ownership of data. . . . Blockchain makes sure that you have full ownership of your data . . . ."); Mark van Rijmenam, *How Blockchain Will Give Consumers Ownership of Their Data*, MEDIUM (July 5, 2019), https://markvanrijmenam.medium.com/how-blockchain-will-give-

B. *Scholarly Proposals*

In academia, the idea of property has repeatedly been proposed as a protection mechanism that could forbid extracting information from data subjects without their consent, hence protecting their privacy.[38]

Property, the argument goes, would allow for a market for personal information in which each data subject could negotiate with firms regarding which uses they are willing to allow with regard to their personal information and for what compensation.[39] By becoming owners of their personal information, according to the argument, data subjects would be able to extract more compensation for its release than they would under a no-property regime, and they would receive compensation for the expected privacy cost associated with each information disclosure.[40] Lawrence Lessig famously promoted the idea of privacy as a form of property rights over data to reinforce people's rights over them.[41]

---

consumers-ownership-of-their-data-3e90020107e6 (last visited Nov. 8, 2021) ("Blockchain is set to change data ownership.").

38 *See, e.g.*, Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2416 (1996); Corien Prins, *When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?*, 3 SCRIPTED 270, 271 (2006) ("With the growing economic importance of services based on the processing of personal data, it is clear that ownership rights in personal data become the key instrument in realizing returns on the investment."); Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113, 1123 (2016) (proposing that privacy law can be seen as property entitlements); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2076–94 (2004) (proposing a property-style approach to regulating personal information).

39 Kenneth C. Laudon, *Markets and Privacy*, 39 ASS'N COMPUTING MACH. 92, 99 (1996) (proposing a "National Information Market" where "information about individuals is bought and sold at a market clearing price"); Murphy, *supra* note 38; Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 62–64 (1999) [hereinafter Lessig, *Architecture of Privacy*]; Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 5 (1996) (discussing a "primary information market" and a "secondary information market"); LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 85–90, 160 (1999) [hereinafter LESSIG, CODE: AND OTHER LAWS]; Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1, 10 (2011) (arguing that this would mitigate the harm from "information pollution"); Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMMS. & TECH. L. REV. 367, 380–84 (2012) (focusing on health privacy); Jim Harper, *Perspectives on Property Rights in Data*, AM. ENTER. INST. (Aug. 8, 2019), https://www.aei.org/technology-and-innovation/perspectives-on-property-rights-in-data (last visited Nov. 18, 2021).

40 *See* Prins, *supra* note 38, at 271 ("[M]arket-oriented mechanisms based on individual ownership of personal data could enhance personal data protection. If 'personal data markets' were allowed to function more effectively, there would be less privacy invasion.").

41 Lawrence Lessig, *Privacy as Property*, 69 SOC. RSCH. 247, 261 (2002) (arguing that it would "allow individuals to differently value their privacy").

More recent proposals tend to suggest some altered version of property to obtain a better fit with the goals of privacy. The recent concept of self-sovereign identity, for example, is aimed at users having complete ownership, and therefore control, over their digital identities.[42] Leon Trakman, Robert Walters, and Bruno Zeller argue for intellectual property protection of personal data, highlighting that intellectual property encompasses attributes of both property and contract law.[43] Lauren Scholtz and Timothy Sparapani, separately, argue for quasi-personal-property protection.[44] Jeffrey Ritter and Anna Mayer suggest regulating data as a new class of property, proposing that regulation of digital information assets and clear concepts of ownership can be built upon existing legal constructs—in particular, property rules.[45]

In one of its most recent permutations, data property exists under the pay-for-privacy movement.[46] Under this movement, there is one element added: The bargaining process triggered by property should lead to financial consideration for personal data. Their underlying idea is that consumers should financially benefit from some proportion of the profits that companies obtain by using their data.[47] While building on property, these proposals contain a slight deviation from usual conceptions of private ordering in mandating what type the consideration in the exchange should be.

Related to the above, the latest academic proposal along property lines is Glen Weyl and Eric Posner's data as labor idea. Contrasting data as labor with data as capital, they call for recognizing the production of

---

42 JEROEN VAN DEN HOVEN, MARTIJN BLAAUW, WOLTER PIETERS & MARTIJN WARNIER, PRIVACY AND INFORMATION TECHNOLOGY (Edward N. Zalta ed., 2019).

43 Leon Trakman, Robert Walters & Bruno Zeller, *Is Privacy and Personal Data Set to Become the New Intellectual Property?*, 50 INT'L REV. INTELL. PROP. & COMPETITION L. 937, 951–52 (2019) (adding that "a constrained conception of IP rights can assist in reconciling principles of contract and general property"); *see also* Will Rinehart, *The Law & Economics of "Owning Your Data,"* AM. ACTION F. (Apr. 10, 2018), https://www.americanactionforum.org/insight/law-economics-owning-data [https://perma.cc/Q723-YS8Q].

44 Scholtz, *supra* note 38, at 1123 ("Privacy should be understood as a quasi-property interest. Courts can handle privacy interests in similar ways as the other members of the quasi-property class."); Timothy D. Sparapani, *Putting Consumers at the Heart of the Social Media Revolution: Toward a Personal Property Interest to Protect Privacy*, 90 N.C. L. REV. 1309, 1313 (2012).

45 Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 260–76 (2018) (discussing the particulars that regard implementing their proposal).

46 *See, e.g.*, Casey Quackenbush, *If You Want an Ad-Free Facebook You're Going to Have to Pay for It, Says Sheryl Sandberg*, TIME (Apr. 6, 2018, 2:38 AM), https://time.com/5230506/facebook-pay-ad-free [https://perma.cc/HWB4-4QJA].

47 Elvy, *supra* note 4, at 1400–28 (showing that pay-for-privacy models turn privacy into a tradeable product).

data as labor that is done for companies that acquire such data, describing it in ownership terms.[48] The personal data that companies profit from is produced and provided by the people to whom that information refers, who are not on those companies' payroll.[49] Data as Labor sees personal data "as user possessions that should primarily benefit their owners."[50] Accordingly, Weyl and Jaron Lanier argued that, because data is a form of labor, taking it without compensation is a form of labor exploitation.[51]

C. *The Descriptive View*

In addition to these normative proposals, one often encounters the descriptive statement of "I own my data" in non-technical spaces. European Commissioner for Competition, Margrethe Vestager, for example, stated that "we all own our data. But . . . we give very often a royalty-free license for the big companies to use our data almost to [do] whatever."[52] Canadian businessman Jim Balsillie, similarly, has argued in Parliament that, due to the effects of the European Union General Data Protection Regulation (GDPR),[53] people have personal ownership of their data, and such data ownership must be woven into a national

48 POSNER & WEYL, *supra* note 5, at 209–33, 245 (including in the proposal both personal and non-personal information and stating, for example, that "[g]overnments would have to ensure that individual digital workers have clear ownership rights over their data . . . [and] the right to freely associate to form data labor unions").

49 *Id.* at 209–33 (adding that "[p]eople's role as data producers is not fairly used or properly compensated" and introducing the concept of "technofeudalism," reminiscent of the property concept of feudalism in which lords take advantage of serfs' land labor and agricultural output).

50 Imanol Arrieta-Ibarra, Leonard Goff, Diego Jiménez-Hernández, Jaron Lanier & E. Glen Weyl, *Should We Treat Data as Labor? Moving Beyond "Free*,*"* 108 AEA PAPERS & PROC. 38, 39 (2018).

51 Lanier & Weyl, *supra* note 26 (proposing the establishment of "mediators of individual data," which operate similarly to data trusts, and tying it to the idea of data dignity).

52 Jennifer Baker, *Vestager on the Intersection of Data and Competition*, IAPP (Oct. 30, 2018), https://iapp.org/news/a/vestager-on-the-intersection-of-data-and-competition/ [https://perma.cc/6VPT-7D7S]; *see also* Kalinda Basho, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CALIF. L. REV. 1507, 1526 (2000) ("Under current law, 'the ownership right to personal information is given to the collector of that information, and not to the individual to whom the information refers.'").

53 Council Regulation 2016/679, 2016 O.J. (L 119) [hereinafter GDPR].

data strategy.[54] These appear frequently, from overheard conversations on the bus to Reddit.[55]

These blanket descriptive statements that privacy law grants property over personal data are incorrect.[56] In Teresa Scassa's words, "the control provided under data protection laws falls short of ownership."[57]

However, privacy law does contain some property-like elements.[58] The same is true of most proposed bills; as Julie Cohen notes, "none of the bills recently before Congress purports, in so many words, to recognize *property* rights in personal data. Even so, almost all adopt a basic structure that is indebted to property thinking."[59] For example, consent is a central element of all federal privacy bills currently before Congress, as it is in some state acts such as the California Consumer Privacy Act (CCPA), the Colorado Privacy Act, and Virginia's CDPA.[60]

---

54 STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS, ETHI 106, EVIDENCE (Can. 2018), https://www.ourcommons.ca/Content/Committee/421/ETHI/Evidence/EV9861805/ETHIEV106-E.PDF [https://perma.cc/LM5S-6UMF].

55 *See, e.g.*, jmlinden7, Comment to *This Guy Is Selling All His Facebook Data on eBay*, REDDIT (May 30, 2018, 12:56 AM), https://www.reddit.com/r/technology/comments/8n2s04/comment/dzt1uh7/?utm_source=share&utm_medium=web2x&context=3 [https://perma.cc/8SFT-KRRE] ("You do own it. And in exchange for using facebook's services you give them the right to sell it."); DisRuptive1, Comment to *Reddit, Why Is It So Bad that My Data Is Being Sold or Stolen by Mega Corporations?*, REDDIT (May 3, 2018, 1:49 AM), https://www.reddit.com/r/NoStupidQuestions/comments/8gnzx0/reddit_why_is_it_so_bad_that_my_data_is_being [https://perma.cc/YWB8-JG43] ("Why is someone else earning money off your data and not you?"); *My "Own Your Data" Project*, REDDIT (Mar. 28, 2019, 4:58 PM), https://www.reddit.com/r/selfhosted/comments/b6o8lu/my_own_your_data_project [https://perma.cc/9QDJ-8HEJ].

56 Nadezhda Purtova, *Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation*, 2 EUR. J. LEGAL STUD. 193, 198–207 (2008) (analyzing this in the context of the European legal system). *See generally* NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (2012) [hereinafter PURTOVA, A EUROPEAN PERSPECTIVE].

57 TERESA SCASSA, DATA OWNERSHIP 13 (2018); *see also* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 463 (2018).

58 *See* Jacob M. Victor, Comment, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 513–15 (2013) (arguing that the GDPR introduces property-like elements through the right to be forgotten and data portability); Thomas E. Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. (forthcoming 2021) (discussing commonalities between cyber trespass law and property law and arguing that treating websites as blackacres violates the First Amendment); Gianclaudio Malgieri, *Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data*, 4 PRIV. GER.—PING 133 (2016) (proposing a taxonomy of control rights to distinguish personal information's property-like characteristics under the GDPR).

59 Julie E. Cohen, *How (Not) to Write a Privacy Law*, *in* KNIGHT FIRST AMEND. INST. 1, 3–4 (2021).

60 CAL. CIV. CODE §§ 1798.140(h), 1798.120, 1798.121(b) (Deering 2019); COLO. REV. STAT. §§ 6-1-1303(5), 6-1-1306(1)(a), 6-1-1308(4), (7) (2021); H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. §§ 59.1-571, 59.1-574(A)(2)).

Data property proposals involve moving the dial further toward these property elements and away from consent-independent restrictions and guarantees.

These descriptive statements show that, because of the property-like elements in current privacy law, data property critiques inform privacy law reform. Under current law, one may transfer rights over personal information through consent, but one may not relinquish all rights regarding personal information. Certain uses of this information—such as use for public shaming—remain prohibited regardless of what people agree to. These restrictions speak against conceptualizing privacy rights as transferable, property-like commodities under current law. While this Article is concerned with normative and not descriptive views on data property, the descriptive view underscores something important: The negative consequences of moving privacy law all the way to consent-based protection can inform whether privacy law should actually move one step toward the opposite direction.

II. WHAT DATA PROPERTY REALLY MEANS

As readers may have noticed, data property proposals have something in common: aiming for people to control their personal information by choosing when to give it away and having the ability to agree on compensation for it. However, this has nothing to do with ownership, and everything to do with transfer.

A. *Rights and Transfer Rules*

Privacy law establishes rights (entitlements) and their corresponding obligations over personal information.[61] But together with establishing rights, the law regulates their transfer.[62] Granting a right and establishing its transactional structure are independent

---

61 This is a broad definition of entitlement, similar to the definition used by Calabresi and Melamed, which only entails that the good (in this case personal information) is owned by someone, and that such person has rights over it. Calabresi & Melamed, *supra* note 8, at 1089; *see also* Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 26 YALE L.J. 710 (1917) (discussing jural opposites and jural correlatives).

62 *See* Alvin K. Klevorick, *On the Economic Theory of Crime*, 27 NOMOS 289 (1985); Alvin K. Klevorick, *Legal Theory and the Economic Analysis of Torts and Crimes*, 85 COLUM. L. REV. 905, 907–09 (1985) [hereinafter Klevorick, *Legal Theory*] (discussing this in the context of criminal law).

operations.[63] Rights' transactional structure determines under which conditions valid exchanges (transactions) over those rights happen.

The law establishes transactional structures by placing transfer rules over rights.[64] Under the Calabresi-Melamed framework, there are three types of transfer rules: property rules, liability rules, and inalienability rules.[65] Rights protected by property rules are transferred with the title-holder's consent and in exchange for a price determined through bargaining.[66] Examples of these are everyday contracts. Rights protected by liability rules are transferred without the title-holder's consent and in exchange for a judicially determined price.[67] Liability rules are used mainly due to high transaction costs of ex-ante bargaining—or an actual bargaining impossibility.[68] For example, if a factory pollutes in breach of environmental law, it will have to pay compensatory damages—not restitution. Rights protected by an inalienability rule are not transferable, and if the transfer somehow takes place, the law sets back or nullifies the transfer to the extent possible.[69] For example, an agreement to sell an organ will be rendered void.[70] Property rules, liability rules, and inalienability rules thus define the transactional structure of the rights they protect, whichever those rights are.[71]

Ownership—also called property rights—is different than property rules. Property rights (ownership) are a set of rights over a thing. Depending on the theory of property one follows, ownership can be conceptualized either as a specific bundle of in rem rights (rights over an object opposable to the whole world) or as dominium over a thing.[72]

---

63 Klevorick, *Legal Theory*, *supra* note 62, at 907–09.

64 *Id.* at 907.

65 Calabresi & Melamed, *supra* note 8, at 1092 (noting that these types are not "absolutely distinct").

66 *Id.* at 1106 (stressing the need to enforce voluntary contracts during transfers).

67 *See, e.g.*, *id.* at 1106–10 (identifying eminent domain as an example of liability rules).

68 *See id.* at 1110 ("[E]fficiency is not the sole ground for employing liability rules rather than property rules.").

69 *Id.* at 1092–93 ("An entitlement is inalienable to the extent that its transfer is not permitted between a willing buyer and a willing seller.").

70 42 U.S.C. § 274e(a).

71 Klevorick, *Legal Theory*, *supra* note 62, at 907 (discussing this in the context of criminal law).

72 Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357, 360–66 (2001) (surveying the traditional "bundle of rights" conception of property); Robert C. Ellickson, *Two Cheers for the Bundle-of-Sticks Metaphor, Three Cheers for Merrill and Smith*, 8 ECON J. WATCH 215, 216 (2011) (arguing that the bundle-of-sticks metaphor "highlights an important feature of a private property system"); *see also* J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. REV. 711, 739–767 (1996) (discussing the bundle of rights view).

In the first position, the set of ownership rights include, for example, the right to use, exclude, sell, possess, subdivide, and lease. In the second position, ownership is a relationship between people in relation to a thing with the key characteristic of omnilaterality.[73]

The right of ownership right (or a property right) is a type of right that can be protected by any transfer rule: property rules, liability rules, or inalienability rules.[74] In contrast—in an unfortunate ambiguity—property rules are a transfer rule based on consent that can be used for any type of right.[75] It may be the case that the more one conceives an entitlement as a property right, the more favorably one will tend to look at property rules and the less that one will tolerate liability rules; for example, the ownership right has few liability rules. Rights over real property are frequently protected by injunctions while contractual rights are frequently protected by damages.[76]

But this correlation does not collapse the conceptual distinction. For example, eminent domain is a liability rule over an ownership right over one's land. Buying the land, on the other hand, is a property rule over the same ownership right. Receiving compensation for environmental harm is a liability rule for something (the environment) over which one does not have ownership; receiving compensation for a bodily injury is also a liability rule over something (one's body parts) that cannot be described as ownership. Subletting a room in an apartment is a property rule over something one does not own. Similarly, transferring rights over data only by consent and on an agreed upon compensation is a property rule over something that one needs not have ownership over. Individuals do not need to hold a property right (ownership) in data in order for the transfer of whichever rights they have over it to occur via property rules.

---

73 *See* Lisa M. Austin, *The Public Nature of Private Property*, *in* PROPERTY THEORY: LEGAL AND POLITICAL PERSPECTIVES 1, 22 (James Penner & Michael Otsuka eds., 2018).

74 Calabresi & Melamed, *supra* note 8.

75 *Id.* at 1092, 1106.

76 Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783, 786 (2007).

		Transfer rule	
		Property rule	Liability rule
Right	Ownership	Sale of a house	Compensation for damage of a car
	Patent	Sale of a patent	Non-commercial use
	Copyright	Transferring copyright	Compulsory license

Table 1: Illustrating the difference between rights and transfer rules

Based on this distinction, one can evaluate whether property rules, liability rules, or inalienability rules are the best way to regulate the transfer of the right to collect, use, or share personal information. While inalienability rules are uncommon and their justifications vary,[77] the law frequently alternates between property and liability rules.[78]

To the extent that the law protects privacy through property rules, the right-holder (data subject) will have the right to decide who can collect, use, or share her personal information and who cannot, hence excluding others from the information. To the extent that privacy interests are protected by liability rules, the right-holder will have a right to be compensated whenever someone accesses, uses, or shares her personal information in a harmful way. Privacy interests are protected by both property and liability rules. The most meaningful question is not which one should be chosen to govern privacy, but rather where on the privacy-to-liability spectrum personal information is best protected.

Consent follows property rules. Broadly speaking, "[u]nderstood as a crucial mechanism for ensuring privacy, informed consent is a natural corollary of the idea that privacy means control over information about oneself."[79] The consent-reliance argument defends the use of property rules for people's personal information, which, under this rule, is collected, processed, and distributed, chiefly based on consent.

---

77 Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931, 969 (1985) (characterizing inalienability as a "second-best response to the messiness and complexity of the world"); Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849, 1903–36 (1987) (evaluating market-inalienability); Lee Anne Fennell, *Adjusting Alienability*, 122 HARV. L. REV. 1403, 1404–10 (2009).

78 Rose-Ackerman, *supra* note 77, at 937–41 (providing efficiency and equity arguments for one transfer rule over another); Radin, *supra* note 77; Fennell, *supra* note 77.

79 Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 44, 57 (Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum eds., 2014).

Placing property rules (due to the ambiguity explained, sometimes misconstrued as ownership) over personal information has been defended on the grounds that it would force a negotiation that would benefit data subjects.[80] Property rules, the argument goes, would allow for a market for personal information in which each data subject could negotiate with firms regarding which types of collection, use, and distribution they are willing to allow with regards to their personal information (or each type of information).[81] Data subjects, moreover, would be able to extract ex-ante compensation for its release,[82] and they would receive compensation for the expected privacy cost associated with each information disclosure.[83] While this appears desirable, there are severe problems with this approach, described in the next Part.

B. *Data Property Is About Transfer, Not About Rights*

When people in politics, the media, the industry, and academia refer to data ownership or to privacy as property, they have largely not proposed to establish a new type of right, but a transfer rule.

Recall that a property right (ownership) is a type of right that can be regulated by any transfer rule.[84] Property-rule protection of personal information amounts to a non-collection default that applies unless consent is given.[85] Property rights often (but not always) have a transactional structure established by property rules. Sometimes, property rights are forcefully "transferred" by liability rules. For example, if you break someone's widget (over which she has personal property) without her consent, as a consequence you must thus pay her a compensation that will be determined by a judge. This amount will not necessarily be the amount that she would have agreed to sell you the widget for.

---

80 *See* LESSIG, CODE: AND OTHER LAWS, *supra* note 39, at 85–90, 159–63; LAWRENCE LESSIG, CODE VERSION 2.0 200–33 (2006).

81 Laudon, *supra* note 39; Murphy, *supra* note 38; Lessig, *Architecture of Privacy*, *supra* note 39; Mell, *supra* note 39; LESSIG, CODE: AND OTHER LAWS, *supra* note 39, at 85–90, 159–63.

82 *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1129 (2000).

83 *See* Prins, *supra* note 38, at 271 ("[M]arket-oriented mechanisms based on individual ownership of personal data could enhance personal data protection. If 'personal data markets' were allowed to function more effectively, there would be less privacy invasion.").

84 *See supra* Section II.A.

85 *See* Calabresi & Melamed, *supra* note 8, at 1092 (explaining that "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").

Arguing that personal data should be subject to a property right could take either of two forms. It could take the form of an argument that personal data should have the same bundle of in rem rights as ownership rights do. Or it could take the form of an argument that personal data should have the main characteristic of ownership: the in rem right to exclude others from the thing over which one has property.[86] In either conception of property, a property right for data would be *numerus clausus*, which is the principle according to which there is a closed form list of property rights.[87] This is not what data property proposals suggest.

Data property proposals emphasize consent as the valve to authorize giving information away. As a consequence, they rely on any agreed-on ex-ante compensation for personal data and not on the particular bundle of rights that is ownership over conventional property (real or personal). In other words, these proposals do not suggest that the right to privacy should be shaped differently—i.e., that a bundle of rights akin to conventional property should be assembled to replace existing privacy rights. They instead suggest that the rights that data subjects hold over their personal information (privacy rights) should not be transferred without their consent or for a socially established compensation, but rather with their consent and for a bargained-for compensation. Transfer by consent, however, is not unique to property rights. Most academic and policy discussions of data property do not discuss the nature of an entitlement (right) but rather how that entitlement is transferred in the marketplace—and that there should be a marketplace for it to start with.

Many of the proposals described above exemplify this idea.[88] Jane Baron discusses data property as a tool to give people control by providing them with choices.[89] Raymond Nimmer and Patricia Krauthhaus argue that "[p]roperty rights in information focus on identifying the right of a company or individual to control disclosure, use, alteration and copying of designated information."[90] The report to

---

86 *See* Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 734–40 (1998) (canvassing perspectives on the right to exclude).

87 Václav Janeček, *Ownership of Personal Data in the Internet of Things*, 34 COMPUT. L. & SEC. REV. 1039, 1041 (2018) (comparing civil and common law and stating that "civilian idea of ownership is an absolute dominion encompassing all the listed rights (*numerus clausus*) over the relevant object; whereas in the common law tradition, ownership includes a variety of different rights over the same property"); *see also* PURTOVA, A EUROPEAN PERSPECTIVE, *supra* note 56, at 1–4.

88 *See supra* Part I.

89 Baron, *supra* note 39, at 415–17.

90 Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property*, 1 INT'L J.L. & INFO. TECH. 3, 5–6 (1993).

the Canadian House of Commons focuses on doing away with non-consented collection and use.[91] Yang's proposal focuses on allowing individuals to "share in the economic value generated by their data,"[92] but the way value is shared depends on the transfer rules and not on the type of right. Likewise, several blockchain proposals focus on control, with statements such as: "Blockchain is set to change data ownership. It will help restore data control to the user by empowering them to determine who has access to their information online."[93] And control depends on the mechanism through which rights are transferred.

This extends to proposals that explicitly use the language of ownership rights. For example, van den Hoven explores ownership as a means of maximizing data subjects' control over their personal information,[94] even though the type of entitlement does little to enhance the right-holder's control over it—the transfer rules do. Ritter and Mayer, similarly, propose a system of ownership to establish control over transfers.[95] But the type of right does not determine whether it is transferred with or without consent—the transfer rules do. Thus, most who claim that privacy rights should transform into ownership rights err in that, without specifying the transfer rule, this identification does not arrive at the kind of protection that they seek.

Some scholars have hinted at this mischaracterization. Cohen's critiques, for example, apply to property rules. Scassa, similarly, has said that "[a]lthough the personal data economy is burgeoning, it appears to be based more on contractual models than on any underlying ownership right in personal information."[96] Václav Janeček and Gianclaudio Malgieri have described the tradability distinctions in

---

91 Standing Committee on Access to Information, Privacy & Ethics, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, 42d Parl., 1st Sess., Ethics Rep. No. 16 (June 2018), https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf [https://perma.cc/F4L9-LGKB] (Canada House of Commons).

92 *Regulating Technology Firms*, *supra* note 26.

93 *See* van Rijmenam, *supra* note 37; *see also* Dickson, *supra* note 6 ("Blockchain makes sure that you have full ownership of your data independent of code that runs the application or the companies, servers, service providers or whoever else that owns the code. You can choose which application will have access to your data and how much of it. You can choose to sell your data or to give free access to it. If you choose to abandon one social media service for another one, you'll carry all your data with you. You'll be setting the terms . . . .").

94 VAN DEN HOVEN, BLAAUW, PIETERS & WARNIER, *supra* note 42, at 3–4 (referring to the concept of "self-sovereign identity").

95 Ritter & Mayer, *supra* note 45, at 261–74.

96 SCASSA, *supra* note 57, at 14 ("While there is no evidence of any ownership rights particular to this context, it is one in which heavy regulation gives individuals some degree of control, in some circumstances, to their personal information, which in turn bolsters the capacity to enter into contracts about access to and use of personal information.").

terms of *res in commercio* and *res extra commercium*, refraining from property language.[97] But the mischaracterization, which is consequential for how one should address these popular reform proposals and how one should address elements of property in privacy law, remains.

The exclusionist conception of property rights, because it focuses on the ability to exclude (and exclusion must be done through an assertion, which expresses consent),[98] rings similar to property transfer rules. This may be a source of confusion. There are, however, two important doctrinal differences. The first is that property rights are in rem and are *numerus clausus*, but transfer rules are not. Data property proposals, as shown above, have neither of these two characteristics. The right to exclude is, in turn, insufficient to transfer the right. For that, one needs the right to alienate—a separate right of the bundle.[99] Conceptualizing data property proposals as suggesting a right as opposed to a transfer rule would thus include two things that the proposals do not argue for (in rem and *numerus clausus*) and lack the main thing that the proposals argue for (control exerted through consent-based alienation).

This in rem characteristic would be patently problematic for personal information. Neither under existing law nor under data property would I have a right, for example, to prevent other people from noticing I bought a banana when I went to the supermarket. But I retain a right under both on whether the store owner can enter the information into a customer data bank to then sell to third parties. Both rights (the one I lack and the one I have) refer to the same information—that I bought a banana. The right is not in rem because it does not accompany the information neither under existing law nor under data property. The right is also not omnilateral, neither under existing law nor under data property, because it depends on the relationship between me and each person regarding the information.

Ensuring a specific means of transfer (i.e., through consent) is the purpose of transfer rules, but it is a corollary of the exclusion right. This conceptual difference is somewhat unimportant for physical objects, where use and transfer are dissociated clearly: I can lend you my soccer ball while retaining my right to exclude you from it. With information,

---

97 Václav Janeček & Gianclaudio Malgieri, *Data Extra Commercium*, *in* DATA AS COUNTER-PERFORMANCE—CONTRACT LAW 2.0? (Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer eds., 2020).

98 Merrill & Smith, *supra* note 72, at 360–66 (defending the exclusionist view).

99 JOHN G. SPRANKLING, UNDERSTANDING PROPERTY LAW 4–5 (2d ed. 2008) (noting that the right to exclude and right to transfer are different sticks in the bundle).

transfer and use get muddled:[100] letting Google use my personal information strikes similar to transferring rights over my personal information to Google. Because use and transfer are muddled in personal information, distinguishing the exclusion right in the bundle of rights that is ownership from property rules for transfer is more important than it is for physical objects, as it is needed to prevent abuses.

In sum, when people have proposed establishing property over data, they have discussed the implications of having data protected solely by property rules, and not necessarily by ownership. One can see this from the language used in scholarship, policymaking, industry, and media—in particular due to the emphasis placed on consent. The view is usually criticized as *the view that people should have an ownership right over data*, but the view is better understood as *the view that people should have a right over their data, whatever kind of right it is, that is protected by property rules*. As the next two Parts explain, this view is objectionable on different grounds.

C. *Inadequate Goal*

Data property, which seeks to promote data subjects' control over personal information, has been criticized for pursuing the wrong goal.[101] This is because privacy is about more than individual control. As Lisa Austin argues, even Alan Westin, often read as the paradigmatic defender of privacy as control, does not support a narrow, control-only definition of privacy.[102]

Ultimately, privacy is necessary for protecting people's autonomy. A lack of privacy can lead an individual to feel that they are under surveillance or scrutiny by others.[103] As a result, their spectrum of thoughts and behaviors may be tailored to those that they perceive others consider acceptable, thereby limiting their freedom to develop as an autonomous person.[104] The importance of privacy for autonomy

---

100 Helen Nissenbaum, *Must Privacy Give Way to Use Regulation?*, *in* DIGITAL MEDIA AND DEMOCRATIC FUTURES 255, 264–69 (Michael X. Delli Carpini ed., 2019) (indicating that the distinction between data collection and use has fuzzy boundaries and leads to slippery slopes).

101 *See, e.g.*, Cohen, *supra* note 10, at 1377.

102 Lisa M. Austin, *Re-reading Westin*, 20 THEORETICAL INQUIRIES L. 53, 58–63 (2019) (discussing how Westin also understands privacy in terms of a condition's experience).

103 *See* Lisa Austin, *Privacy and the Question of Technology*, 22 L. & PHIL. 119, 129, 140 (2003) (explaining how this would affect reasonable expectations of privacy).

104 Stanley I. Benn, *Privacy, Freedom and Respect for Persons*, *in* PRIVACY 1, 6–7 (J. Roland Pennock & John W. Chapman eds., 1971).

leads privacy to be central to citizenship.[105] Privacy, thus, is more than individual control over information.

Cohen argues that property cannot support a broad conception of the protection of privacy.[106] Data property would lead individuals to focus, above all things, on their "surplus in the marketplace," which is contrary to U.S. constitutional values, which establish "robust privacy protection for thought, belief, and association."[107] She indicates that property is an undesirable means of privacy protection to the extent that the thing that is owned (data) is equated with tradability.[108] But, unlike other market goods, personal information is part of people's personhood.[109] Relatedly, data property has been said to raise constitutional issues, particularly in terms of speech.[110]

Protecting privacy beyond a market for personal information is crucial for respecting individuals.[111] Elettra Bietti, for example, argues that "ownership creates a market over data as a commodity and entails a specific kind of harm: that of severing the self from personal data as an object, allowing monetization and trade over such object, and obscuring the losses in human dignity or integrity that result."[112] For that reason, she argues that shaping the data economy through transfer and acquisitions is reductive.[113] Jane Bambauer, similarly, demonstrates that data ownership and a market to disseminate personal information would not work because personal information is nonrivalrous and its value is difficult to predict.[114]

---

105 Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912–18 (2013) (analyzing the interplay between privacy and systems of surveillance and arguing that freedom from surveillance is key to the practice of informed and reflective citizenship).

106 Cohen, *supra* note 10, at 1380.

107 Julie E. Cohen, *Privacy, Autonomy and Information*, *in* CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 1, 4 (2012) (adding that propertizing privacy shields surveillance from public scrutiny because the marketplace rubberstamps it).

108 Cohen, *supra* note 10, at 1384.

109 *Id.* at 1378 (stating that "the understanding of ownership that applies to, say, cars or shoes just seems a crabbed and barren way of measuring the importance of information that describes or reveals personality").

110 Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1294 (2000) ("Property rights in any sort of information raise significant policy and free speech issues. Facts are basic buildings blocks: building blocks of expression; of self-government; and of knowledge itself.").

111 Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559, 582–85 (2015) (linking this idea to sociology).

112 Elettra Bietti, Locked-in Data Production: User Dignity and Capture in the Platform Economy 19 (Oct. 14, 2019) (unpublished manuscript) (on file with SSRN).

113 *Id.*

114 Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 224 (2012).

Equating data with tradability is what property rules—but not property rights—do. Together with these other critiques, Cohen shows, in other words, that data property proposals pursue the inadequate goal of individual control. Because Cohen's critique focuses on the problems of tradability, it problematizes the application of property rules to personal data. As I showed above, this is what data property proposals suggest. These critiques therefore apply to data property proposals (as reframed), and not only to the strawman of creating ownership rights over personal data.

Privacy scholars have correctly argued that data ownership faces important problems in critiques that extend both to ownership rights and to property rules. Viewing data property for what it is allows one to see two additional things: that data property inherits the problems of consent and that it also defeats itself.

III. WHY DATA PROPERTY IS INEFFECTIVE: OLD REASONS APPLIED TO NEW GROUND

Once one understands data property proposals for what they are—relying on people to self-protect and compensate privacy based on agreements, independently of eventual harms caused—one can see that several criticisms directed at privacy law's reliance on individual consent also apply to data property, exposing equivalent flaws.

Because of its focus on trade (relying solely on property rules), data property creates three structural problems in the protection of privacy rights. First, it inherits the notice and choice model's asymmetric information problem. Second, and relatedly, it becomes ineffective at protecting privacy due to unequal bargaining positions. Third, it under-protects personal information derived from data aggregation (inferred information). These structural problems are discussed in the following three Sections.

A. *Asymmetric Information*

The last Part showed that data property is not concerned with the type of rights held over personal information but rather with transferring them through consent.[115] For that reason, the limits of the notice and choice paradigm translate into data property. Although this Article is not about the benefits and limits of consent in privacy, notice

115 *See supra* Section II.B.

and choice's asymmetric information problem is relevant because data property inherits it.[116]

There is, at a broad level, an information asymmetry problem between data subjects and data processors that makes consumers vulnerable.[117] Data subjects lack the technical knowledge necessary to sufficiently understand terms and conditions.[118] Moreover, understanding them, let alone bargaining over them, would take an enormous amount of time.[119]

Solon Barocas and Helen Nissenbaum have said that "[b]ig data extinguishes what little hope remains for the notice and choice regime."[120] While many call for more companies to implement consumer privacy notices as a way to increase transparency,[121] others suggest that notices are ineffective at increasing consumer awareness of how their personal information is managed, even if they are simplified

116 *See, e.g.*, Elena Gil González & Paul de Hert, *Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data—An Analysis of GDPR Provisions and Principles*, 19 ERA F. 597, 600 (2019) ("Consent has become a cornerstone of data protection across the EU. However, reliance on consent is not always the best option. Indeed, it is only appropriate if the controller can offer genuine choice, control and responsibility to individuals over the use of their personal data.").

117 Schwartz, *supra* note 38, at 2080; *see* TONY VILA, RACHEL GREENSTADT & DAVID MOLNAR, WHY WE CAN'T BE BOTHERED TO READ PRIVACY POLICIES: MODELS OF PRIVACY ECONOMICS AS A LEMONS MARKET 3 (2003) (arguing that the information asymmetry leads to an adverse selection problem); *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) ("A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched.").

118 Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 172–74 (discussing the sustainability of the market-based manipulation argument); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003–18 (2014) (arguing that the future of market manipulation is one marked with corporations exploiting the limits of each consumer's ability to pursue their own self-interests).

119 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & POL'Y FOR INFO. SOC'Y 543, 544 (2008).

120 Solon Barocas & Helen Nissenbaum, *Computing Ethics Big Data's End Run Around Procedural Privacy Protections*, 57 COMMC'NS ACM 31 (2014) (also stating that "the problem we see with informed consent and anonymization is not only that they are difficult to achieve; it is that, even if they were achievable, they would be ineffective against the novel threats to privacy posed by big data"); *see also* Strandburg, *supra* note 13, at 165–72 (arguing that neither notice and choice nor a more robust consent regime can overcome the basic problems of behavioral advertising business models).

121 M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1047–59 (2012) (proposing visceral notices for privacy); Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory System*, 34 FLA. ST. U. L. REV. 1089, 1092–93 (2006) (noting the provision of notices as a common method for regulation); William M. Sage, *Regulating Through Information: Disclosure Laws and American Healthcare*, 99 COLUM. L. REV. 1701, 1715–20 (1999) (explaining the provision of notices as a common method for regulation in medicine).

and even if people read them.[122] Empirical evidence has shown that simplifying disclosures has no effect on consumer awareness, suggesting that language complexity is not the main driver.[123] Moreover, other empirical work suggests that the language used in a privacy policy is irrelevant, which in turn suggests that consumers do not react to different kinds of language.[124]

This limitation on the usefulness of notices may be due to information overload.[125] That is, it may be the case that the reason why notices are rarely effective is that, no matter how simply formulated or visible they are, there are too many cognitive steps between the information disclosed (e.g., geolocation tracking) and the information that is useful (e.g., does anyone know where I go and who I spend time with?).[126] For example, while people do not respond to privacy policies, they have been shown to more easily respond to and understand information conveyed by design choices.[127] Information overload is worsened by the problem of data aggregation discussed below because one of the main drivers of consumers' difficulty to estimate costs is anticipating how information aggregates.[128]

Beyond descriptive criticisms about the effectiveness of the notice and choice approach, it has received normative criticisms based on the dynamic between companies, the State, and individuals.[129] From a

---

122 Kirsten Martin, *Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online*, 45 J. LEGAL STUD. S191, S204–06 (2016) (using a vignette study to show that formal privacy notices reduce consumer trust in a website); *see also* SOLON BAROCAS & HELEN NISSENBAUM, ON NOTICE: THE TROUBLE WITH NOTICE AND CONSENT, *in* PROCEEDINGS OF THE ENGAGING DATA FORUM (2009); McDonald & Cranor, *supra* note 119, at 544 (showing the time and energy needed to comprehend privacy policies); Susanna Kim Ripken, *The Dangers and Drawbacks of the Disclosure Antidote: Toward a More Substantive Approach to Securities Regulation*, 58 BAYLOR L. REV. 139, 185–203 (2006) (explaining the limits of a disclosure-based policy generally and suggesting direct conduct regulation through the example of securities).

123 Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. LEGAL STUD. S41, S44 (2016) (finding that best-practice simplification techniques have little or no effect on respondents' comprehension of disclosures).

124 Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S76–83 (2016) (testing language in privacy policies).

125 Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1475, 1489–90 (2018).

126 *Id.*

127 Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 113–14 (2018) (characterizing design's effect as "powerful"); Ari Ezra Waldman, *A Statistical Analysis of Privacy Policy Design*, 93 NOTRE DAME L. REV. ONLINE 159, 163–71 (2018) (discussing a survey's findings).

128 *See infra* Section III.C.

129 *See* Lisa M. Austin, *Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA*, 56 U. TORONTO L.J. 181, 188–94 (2006) (presenting the case for being

structural perspective, the approach has been criticized for over-focusing on each individual ("it is up to me to decide what information about me I want to share and with whom").[130] As a consequence, the argument goes, the approach insufficiently addresses legitimate countervailing interests. Sometimes, privacy interests can yield to other interests—such as containing a pandemic. The consent-based approach addresses this by formulating exceptions for them—such as public interest exceptions. But the formation of obligations for entities who must obtain consent to collect or process personal information in a way that is context-independent fails to appropriately recognize interests that are not the individual's.[131]

Because data property depends on consent and control, the asymmetric information criticism of the notice and choice system extends to the reliance on consent by property rules.[132]

B. *Unequal Bargaining Positions*

A second limitation of data property is that it assumes that data subjects' expressions of consent means that they are able to manage their privacy risks. Even if they are fully informed, data subjects will rarely be able to manage their privacy risks because of the unequal bargaining power between them and companies.

Due to the type of interactions in which privacy policies are involved, where data subjects have limited options, it is at least questionable to believe that reinforcing property rules would improve data subjects' bargaining position.[133] Under property rules, data subjects frequently face a take-it-or-leave-it option between either using a product and giving their personal information for free, or not using the

skeptical of notice and choice); Lisa M. Austin, *Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices*, 44 CAN. BUS. L.J. 21, 24–25 (2006) (summarizing the consent-based model's deficiencies).

130 Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131, 141 (Austin Sarat ed., 2014).

131 *Id.* at 7–9.

132 *See* Richards & Hartzog, *supra* note 12, at 444 (explaining that the narrative of control feeds from the narrative of privacy self-management); *see also* Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1184 (2017).

133 Sarah Spiekermann, Alessandro Acquisti, Rainer Böhme & Kai-Lung Hui, *The Challenges of Personal Data Markets and Privacy*, 25 ELEC. MKTS. 161, 165–67 (2015); *see also* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020) (discussing power asymmetries between data subjects and companies).

product at all.[134] If they need to use the service, for example, because using it is part of normal social life and therefore costly to opt-out of it, such as with email or a cellphone provider, this consent is not given freely.[135]

This relates to the idea of privacy self-management, under which people manage their own privacy in making decisions about when and how to give away their personal information.[136] The privacy self-management model is predicated on the false premise that informed and rational individuals will make appropriate decisions as to the use and collection of their personal data.[137] This model fails to address the unequal bargaining positions between data subjects and information intermediaries, as well as the data aggregation problem explained below.

It is impossible for data subjects to properly assess the risks involved in disclosing their personal information in the digital environment.[138] Data subjects cannot assess the risks of disclosing because they do not always know how their data will be used and what can be done with it.[139] Some also argue that data processors even have economic incentives to mislead data subjects, which adds to the problem.[140] As Maurice Stucke and Ariel Ezrachi explain: "Under the . . . opaque system, there's no way of knowing whether we're getting a fair deal. We have little idea how much personal data we have provided, how it is used and by whom, and what it's worth."[141] The costs of assessing risks when providing consent are enormous.[142]

---

134 *See* Samuelson, *supra* note 82, at 1162–63 (describing the contractual elements of this relationship).

135 Bietti, *supra* note 112 (manuscript at 29) ("[O]pting for market or property-based mechanisms, leaves private platform companies with too much objectionable power over their users and too much power to interfere with their basic human interests.").

136 *See* Solove, *supra* note 12, at 1882–83 (introducing privacy self-management and consent's structural problems in privacy).

137 *Id.* at 1883 (noting that "[p]rivacy self-management envisions an informed and rational person who makes appropriate decisions about whether to consent to various forms of collection, use, and disclosure of personal data").

138 *See* Bietti, *supra* note 112 (manuscript at 19) ("[I]t is likely that an ownership regime would benefit the most informed and educated of data producers to the detriment of the helpless and misinformed, who could easily be tricked into selling their data at lower than market value."); *see also* Samuelson, *supra* note 82, at 1128, 1145 (noting that commentators think the law should supply corrective measures).

139 Cofone & Robertson, *supra* note 125, at 1475, 1489–90 (discussing information overload and aggregation).

140 Trakman, Walters & Zeller, *supra* note 43, at 950.

141 MAURICE E. STUCKE & ARIEL EZRACHI, COMPETITION OVERDOSE: HOW FREE MARKET MYTHOLOGY TRANSFORMED US FROM CITIZEN KINGS TO MARKET SERVANTS 435 (2020).

142 Samuelson, *supra* note 82, at 1145 (adding that while most objects that are sold can be replaced, one cannot replace personal data once it is disclosed).

Accordingly, Neil Richards and Woodrow Hartzog argue that digital consent is only valid when choices are infrequent (to prevent choice overload), the potential harms are easy to imagine (so that consent is meaningful), and consumers have reasons to choose consciously and seriously (so that consent is real).[143] And digital consent over privacy rarely meets these conditions.[144] It is difficult to believe in this context, even with the efforts on reinforcing meaningful consent, that data subjects could make informed and welfare-enhancing choices.[145]

C. *Aggregated and Inferred Personal Data*

Another problem is that personal information is inferred by aggregating data; that is, by compiling different types of information provided by the data subject, perhaps to different companies, at different times. This information is under-protected by property rules. This is because risks of aggregation are impossible to estimate, as scaling effects make the sum of disclosures unequal to constituent parts of disclosures.

Even if there were adequate information and no obstacles to how freely consent is given, data subjects under data property would receive ex-ante compensation only for providing consent for each piece of information released to each data collector. However, they would not have ex-ante compensation for the inferred information, which is more valuable and potentially more harmful.[146]

Taken individually, most data points shared might not even be valuable enough to induce companies and data subjects to bargain over

143 Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1476–91 (2019).

144 *Id.* at 1498–1502.

145 *See* Strandburg, *supra* note 13, at 95 ("In a functioning market, payment of a given price signals consumer demand for particular goods and services, transmitting consumer preferences to producers. Data collection would serve as 'payment' in that critical sense only if its transfer from users to collectors adequately signaled user preferences for online goods and services."); Nadezhda Purtova, *Do Property Rights in Personal Data Make Sense After the Big Data Turn?*, 10 J.L. & ECON. REG. 64, 72–73 (2017).

146 Barocas & Nissenbaum, *supra* note 120, at 32 (discussing the harm aggregated information poses); Solove, *supra* note 12, at 1889–91; Strandburg, *supra* note 13, at 98 ("[I]mperfect consumer information about the potential harms of data collection, company data practices, and means to mitigate data collection combine with the properties of information aggregation and with common behavioral economics concerns to undercut the market's responsiveness to consumer preferences.").

them.[147] But, combined, the same data points present high risks to users.[148] And the way that information aggregates, as well as how high these costs are, are extremely difficult for data subjects to anticipate.[149] People lack protection for the risks of disclosing personal data if they are given small compensations for each disclosure while they face high expected harms for them in aggregation.[150]

Two recent cases illustrate this dynamic. In *Meyers v. Nicolet Restaurant*, a restaurant allegedly violated the Fair and Accurate Credit Transactions Act (FACTA) by printing the expiration date of a credit card on a sales receipt.[151] In *Kirchein v. Pet Supermarket*, a supermarket printed more than five digits of credit card numbers on customers' receipts, which is a violation of prohibitions on printing more than the last five digits of the credit card number or expiration date on the receipt provided to the customer.[152] In both cases, the plaintiffs alleged that the company increased the risk that the customers' identity would be compromised, for example through identity theft. Printing a full credit card number instead of the last four digits, or printing the expiration date together with the last four digits, may seem harmless in isolation. But, if businesses are not sanctioned for breaching FACTA in such a way and a malicious actor can hack the systems of a few restaurants, because of the aggregation problem, it may be easy for them to duplicate credit cards. If that happens, it will be difficult for customers to trace back the duplicated credit cards to the aggregation

147 *See, e.g.*, Emily Steel, Callum Locke, Emily Cadman & Ben Freese, *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth [https://perma.cc/CZ2W-BRMZ]; Ignacio Cofone, *Why Paying for Facebook Won't Fix Your Privacy*, VENTUREBEAT (Apr. 17, 2018, 5:10 PM), https://venturebeat.com/2018/04/17/why-paying-facebook-wont-fix-your-privacy [https://perma.cc/Q9F5-46JX].

148 Strandburg, *supra* note 13, at 134–41 (discussing how "data accumulated for behavioral targeting of advertisements can be (and is) used not only to target ads for particular products to particular consumers but also to facilitate price discrimination").

149 Strandburg, *supra* note 13, 130–52 ("[I]t is nearly impossible for a consumer to estimate the increment in expected harm associated with a given instance of data collection."); Cofone & Robertson, *supra* note 125.

150 This aggregation problem relates to the dignity-based criticism of data as property. *See* Bietti, *supra* note 112 (manuscript at 13) ("[S]ubjecting and devolving large amounts of personal data to market forces could be said go against our dignity . . . .").

151 Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724, 725 (7th Cir. 2016) ("Meyers was given a copy of his receipt after dining at Nicolet . . . . He noticed that Nicolet's receipt did not truncate the expiration date, as the FACTA requires.").

152 Kirchein v. Pet Supermarket, Inc., 297 F. Supp. 3d 1354, 1356 (S.D. Fla. 2018) ("Kirchein filed a putative class action alleging that the Defendant violated the Fair and Accurate Credit Transactions Act ('FACTA'), which prohibits printing 'more than the last five digits of the credit card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.'").

of different pieces of extra credit card information from the different restaurants.[153]

Another extension of the inference problem is that personal information is inferred not only from the information that each individual releases but also from information provided by or taken from others. Data about different people are routinely combined.[154] My consent to collection and usage of data about me can be used to inflict harm on others when combined with their own shared information.[155] Consent of any person becomes irrelevant as one aggregates people to the dataset and infers, probabilistically, personal information about each person based on what was disclosed by others.[156] Under a data property model, each individual is a prisoner of other people's choices.

That has led some to characterize personal data as a public good.[157] In other words, information is not a distinct commodity because it can be held by several agents at the same time. Every decision about personal data has spillover effects on others.[158] This has led some commentators to characterize personal information as a commons, where personal information exchanges generate negative externalities towards others who are impacted by the exchange indirectly in a way that is not captured by property rules.[159] And information is relational, in that it relates to more than one person. Examples of these characteristics can be as simple as a group photo or as complex as a database to train a machine learning algorithm. No data is only about

---

153 Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 756–58 (2018) ("A problem is that fraud may not surface until after an identity thief combines leaked personal data with other information.").

154 *See* Bietti, *supra* note 112 (manuscript at 7, 19) ("[A] lot of data is created unintentionally . . . as part of a diffuse system that captures it without a specific purpose for doing so.").

155 Przemyslaw Palka, *Data Management Law for the 2020s: The Lost Origins and the New Needs*, 68 BUFF. L. REV. 559, 595–602 (2020) (adding that, for that reason, I lack a moral right to give such consent).

156 Barocas & Nissenbaum, *supra* note 120 (explaining consent becomes meaningless as someone aggregates people to the data); Purtova, *supra* note 145 (explaining this in terms of network effects).

157 *See, e.g.*, Schwartz, *supra* note 38, at 2084; Ignacio N. Cofone, *The Dynamic Effect of Information Privacy Law*, 18 MINN. J.L. SCI. & TECH. 517, 530–31 (2017); Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 421–33 (2015).

158 Lanah Kammourieh et al., *Group Privacy in the Age of Big Data*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 37, 52–55 (Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., 2017); Ugo Pagallo, *The Group, the Private, and the Individual: A New Level of Data Protection?*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 159, 161–64 (Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., 2017).

159 Schwartz, *supra* note 38, at 2084–90; Nadezhda Purtova, *Property Rights in Personal Data: Learning from the American Discourse*, 25 COMPUT. L. & SEC. REV. 507, 519 (2009); Spiekermann, Acquisti, Böhme & Hui, *supra* note 133, at 162; Fairfield & Engel, *supra* note 157.

one person.[160] These characteristics make personal information unfit for in rem rights and for individual-consent-based property rules. A consequence of our information's informativeness about other people is that property itself becomes difficult to allocate appropriately, as several data subjects may have a claim over a single piece of information.[161] Trying to square data property, which would give exclusion rights to each "owner," with something as simple as a group photo, shows that stating that someone "owns" data is at odds with the idea that privacy is about governing appropriate information flows[162]—the power to exclude cannot be given to everyone involved in the information.

An extension of this problem is the under-protection of de-identified data.[163] Privacy statutes do not protect data without identifiers. But so-called anonymous datasets hold enormous power, and they can cause group harms. Even data that is kept anonymized is informative of individuals in the aggregate. Thus, it can be harmful to individuals because it is informative about groups that they belong to, allowing inferences for members of such groups.[164] For example, if a company has information about people's sexual orientation and it also has aggregated probabilistic information about preferences and behavior of queer individuals, then it knows more about each queer individual than if it only had the former.

Moreover, data can always be re-identified.[165] Data property cannot require compensation upon re-identification because its protection exists only at the moment of transfer. Consent-based rules, therefore, under-protect data that are obtained while being anonymized, which then can be de-anonymized, becoming harmful.

---

160 Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 4 EUR. DATA PROT. L. REV. 492, 493 (2020) ("[T]he FIPs approach never considered that future consumers and citizens might create so much data and have so many commercial and government accounts that informational self-determination could become impossible.").

161 Spiekermann, Acquisti, Böhme & Hui, *supra* note 133, at 163.

162 HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 67–126 (2010); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 131–36 (2004).

163 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716–31 (2010) (discussing the ease of reidentification).

164 Linnet Taylor, Bart van der Sloot & Luciano Floridi, *Conclusion: What Do We Know About Group Privacy?*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 225, 225–29 (Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., 2017) (explaining that anonymized data is informative of preferences, behavior, population mobility, urban dynamics, among others); *see also* Brent Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, 30 PHIL. & TECH. 475, 475–80 (2017).

165 Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information,"* 53 COMMC'NS ACM 24, 24–26 (2010).

This includes both the privacy harm that re-anonymization involves per se and the consequential harms that can accrue from it.

From a process viewpoint, the idea of data as labor diverges here because it validates control over inferred data by data aggregators by arguing that, because they invested labor into creating it, they are more deserving of having control.[166] That is, the lack of protection for inferred data is not a bug but a feature of the data as labor idea. This does not invalidate the aggregation-based normative criticism towards it. Moreover, even under the data as labor idea, most pieces of inferred information that someone contributes to will also have had contributions by others, creating simultaneous claims or at least the curtailing of some property rights by other people's incompatible claims.[167]

Personal data, in other words, is about inferences.[168] Even if it were true that data subjects made informed and free decisions about their data, companies would infer information about them based on the information that they have about others; that is, information that others have consented to disclose but the data subject has not.[169]

In sum, data property would not protect against data aggregation. That is so because it would not provide control over inferred information—created by assembling previously collected information—and would be impossible to allocate appropriately for information that is relational.

* * *

Consent-for-use is the system already in place for privacy,[170] and privacy scholars have shown that it is ineffective. Data property, by placing further weight on consent-for-use, would not improve the status quo. A regime that relies only on property rules would mean that companies would be able to use individuals' data when those individuals consent to the use. But consumers already do this when they

166 POSNER & WEYL, *supra* note 5, at 205–49.

167 Bietti, *supra* note 112 (manuscript at 19).

168 *See* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1049–53 (2018) (explaining how information about someone is inferred probabilistically based on information provided by them and others).

169 Barocas & Nissenbaum, *supra* note 120, at 32 (discussing what we learned from Target's "infamous pregnancy prediction score" incident).

170 *See, e.g.*, CAL. CIV. CODE §§ 1798.140(h), 1798.120, 1798.121(b) (Deering 2019); COLO. REV. STAT. §§ 6-1-1303(5), 6-1-1306(1)(a), 6-1-1308(4), (7) (2021); H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. §§ 59.1-571, 59.1-574(A)(2)).

consent to websites' and apps' terms of service. The ineffectiveness of data property is not theoretical—it is actualized.

IV. WHY DATA PROPERTY IS SELF-DEFEATING

In addition to exacerbating these pre-existing problems,[171] data property contains a fatal flaw: it produces moral hazard. In contrast to existing property criticisms, which show how data property tries to achieve the wrong goal,[172] and newly applicable criticisms, which show that data property is ineffective at protecting people's privacy,[173] the moral hazard problem means that data property is counterproductive at doing the very thing it tries to do: increasing user control.

A. *Moral Hazard in Privacy Law*

1. The Grindr Hazard

In January 2021, queer dating app Grindr faced a historic fine of ten percent of its global turnover by the Norwegian Data Protection Authority.[174] The fine arose from having inadequate consent provisions as to what information it sent to third parties. A take-it-or-leave-it option in its privacy policy, the Authority ruled, was insufficient given the information's sensitivity, which includes sexual orientation and HIV status.[175] Similarly, in *Frank v. Gaos*, Google allegedly leaked information about users' search terms to third parties, providing websites with users' personal information, as well as informing them of the search terms that led users to their website.[176] The plaintiffs alleged that the collection and unauthorized disclosure led to feelings of being

171 *See supra* Part III.

172 *See supra* Section II.C.

173 *See supra* Part III.

174 Finn Myrstad & Øyvind H. Kaldestad, *Historic Victory for Privacy as Dating App Receives Gigantic Fine*, FORBRUKERRÅDET (Jan. 26, 2021), https://www.forbrukerradet.no/news-in-english/historic-victory-for-privacy-as-dating-app-receives-gigantic-fine [https://perma.cc/H5WL-DRLJ] (explaining the Norwegian Data Protection Authority's decision and declaring it as a "milestone in the ongoing work to ensure that consumers' privacy is protected online").

175 *Norwegian DPA: Intention to Issue € 10 Million Fine to Grindr LLC*, EUR. DATA PROT. BD. (Jan. 26, 2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-intention-issue-eu-10-million-fine-grindr-llc_en [https://perma.cc/YAX9-KFBC]; Øyvind H. Kaldestad, *Filing Complaint Against Grindr's Sharing Users' HIV-Status and Sexual Preferences*, FORBRUKERRÅDET (Apr. 3, 2018), https://www.forbrukerradet.no/side/filing-complaint-against-grindrs-sharing-users-hiv-status-and-sexual-preferences [https://perma.cc/D873-YXNQ].

176 Frank v. Gaos, 139 S. Ct. 1041, 1044 (2019).

under surveillance. Why was Grindr and Google users' well-being affected after they had agreed to a policy that authorized both practices? Because of privacy law's moral hazard problem.

Moral hazard takes place when someone (in this case, a company that collects or processes personal data) has incentives to increase risk for someone else (in this case, consumers) because they do not bear the cost of such a risk increase.[177] Although moral hazard is frequently explained in terms of insurance, it is much broader: in economic terms, for the purposes of moral hazard, "'insurance' is provided any time that one party's actions have consequences for the risk of loss borne by another."[178] Particularly, limiting liability falls within that broad conception of insurance.[179]

Legal scholars have proposed solutions for moral hazard across several areas of the law.[180] A common type of moral hazard is the

---

177 *See* PAUL MILGROM & JOHN ROBERTS, *Moral Hazard and Performance Incentives*, *in* ECONOMICS, ORGANIZATION AND MANAGEMENT 166, 166–70, 179, 185–90 (1992) (explaining how moral hazard leads to perverse risk incentives). *See generally* John M. Marshall, *Moral Hazard*, 66 AM. ECON. REV. 880 (1976) (introducing the seminal contribution for moral hazard in economics); David Rowell & Luke B. Connelly, *A History of the Term "Moral Hazard,"* 79 J. RISK & INS. 1051, 1051–58, 1064–69 (2012) (explaining the historical evolution of the term and the differences between its colloquial and economics uses).

178 Tom Baker, *On the Genealogy of Moral Hazard*, 75 TEX. L. REV. 237, 272 (1996).

179 Reinier H. Kraakman, *Corporate Liability Strategies and the Costs of Legal Controls*, 93 YALE L.J. 857, 873–74 (1984); James R. Garven & Steven W. Pottier, *Incentive Contracting and the Role of Participation Rights in Stock Insurers*, 62 J. RISK & INS. 253 (1995).

180 *See, e.g.*, George L. Priest, *A Theory of the Consumer Product Warranty*, 90 YALE L.J. 1297 (1981); Richard S. Higgins, *Products Liability Insurance, Moral Hazard, and Contributory Negligence*, 10 J. LEGAL STUD. 111 (1981); Lawrence Blume & Daniel L. Rubinfeld, *Compensation for Takings: An Economic Analysis*, 72 CALIF. L. REV. 569 (1984); Richard A. Epstein, *Products Liability as an Insurance Market*, 14 J. LEGAL STUD. 645 (1985); Jon D. Hanson & Kyle D. Logue, *The First-Party Insurance Externality: An Economic Justification for Enterprise Liability*, 76 CORNELL L. REV. 129 (1990); Richard J. Butler & John D. Worrall, *Claims Reporting and Risk Bearing Moral Hazard in Workers' Compensation*, 58 J. RISK & INS. 191 (1991); Daniel Keating, *Pension Insurance, Bankruptcy and Moral Hazard*, 1991 WIS. L. REV. 65; Howell E. Jackson, *The Expanding Obligations of Financial Holding Companies*, 107 HARV. L. REV. 507 (1994); Nita Ghei & Francesco Parisi, *Adverse Selection and Moral Hazard in Forum Shopping: Conflicts Law as Spontaneous Order*, 25 CARDOZO L. REV. 1367 (2004); Ronald J. Gilson & Alan Schwartz, *Understanding MACs: Moral Hazard in Acquisitions*, 21 J.L. ECON. & ORG. 330 (2005); Lawrence A. Cunningham, *Sarbanes-Oxley Accounting Issues: Too Big to Fail: Moral Hazard in Auditing and the Need to Restructure the Industry Before It Unravels*, 106 COLUM. L. REV. 1698 (2006); Jonathan Klick & Thomas Stratmann, *Diabetes Treatments and Moral Hazard*, 50 J.L. & ECON. 519 (2007); Karl S. Okamoto, *After the Bailout: Regulating Systemic Moral Hazard*, 57 UCLA L. REV. 183 (2009); Henry Schneider, *Moral Hazard in Leasing Contracts: Evidence from the New York City Taxi Industry*, 53 J.L. & ECON. 783 (2010); Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012); Albert C. Lin, *Does Geoengineering Present a Moral Hazard?*, 40 ECOLOGY L.Q. 673 (2013); Steven L. Schwarcz, *Too Big to Fool: Moral Hazard, Bailouts, and Corporate Responsibility*, 102 MINN. L. REV. 761 (2017); Peter Molk, *Playing with Fire? Testing Moral Hazard in Homeowners Insurance Valued Policies*, 2018 UTAH L. REV. 347; Solomon Miller, *Current Developments 2018–*

principal-agent problem, where the behavior of one party (the agent) affects the well-being of the other party (the principal) and there is asymmetric information about the behavior of the former (the principal has limited knowledge of the behavior of the agent).[181] The agent then has incentives to either invest lower amounts of effort than optimal (which economists call "slack") or act in a way that is beneficial to him but not in the best interest of the principal (which economists call "expropriate").[182]

Moral hazards are what economists call an ex-post information asymmetry problem: it happens after the interaction takes place and because one of the parties (in this case, the consumer) has little information about what the other parties (in this case, the companies) do.[183] If both parties could know in advance and be able to observe the agent's risk-taking behavior following the interaction, they could try to add a contractual clause that internalizes the risk.[184] But one of those parties (in this case, the consumer) is unable to do so because of the information asymmetry.[185]

Because one of those parties (the consumer) does not know when the other party (the corporation) engages in risky behavior, the second party (the corporation) has incentives to take more risk than the first party (the consumer) would agree to.[186] This is a problem in areas where the first party's well-being is affected by the second party's behavior after the interaction. In particular, it is a problem when the second

---

2019: Ending Prosecutor's Moral Hazard in Criminal Sentencing, 32 GEO. J. LEGAL ETHICS 833 (2019); Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71 (2020).

181 *See* John Armour, Henry Hansmann & Reinier Kraakman, *Agency Problems and Legal Strategies*, *in* THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH 29 (3d ed. 2017) (explaining principal-agent problems); Kenneth J. Arrow, *The Economics of Moral Hazard: Further Comment*, 58 AM. ECON. REV. 537, 538 (1968) (introducing moral hazard).

182 Armour, Hansmann & Kraakman, *supra* note 181 (explaining moral hazard's incentive problems in principal-agent problems).

183 Bengt Holmström, *Moral Hazard and Observability*, 10 BELL J. ECON. 74, 74, 80–81 (1979) (discussing the consequence of information asymmetries in the context of optimal deductibles in insurance).

184 Sugato Bhattacharyya & Francine Lafontaine, *Double-Sided Moral Hazard and the Nature of Share Contracts*, 26 RAND J. ECON. 761, 766–75 (1995) (exploring contractual arrangements involving revenue in double-sided moral hazard, including limited possibilities for customizing contractual terms); Eva I. Hoppe & Patrick W. Schmitz, *Hidden Action and Outcome Contractibility: An Experimental Test of Moral Hazard Theory*, 109 GAMES & ECON. BEHAV. 544, 550–57 (2018) (showing in an experimental setting that contractual bargaining is desirable, when possible, to solve hidden action moral hazard).

185 Holmström, *supra* note 183, at 74.

186 Patrick W. Schmitz, *On the Interplay of Hidden Action and Hidden Information in Simple Bilateral Trading Problems*, 103 J. ECON. THEORY 444, 444–47 (2002) (classifying this scenario as "hidden action").

party's care can reduce the amount of harm to the first party, they can control their level of care, their liability does not depend on their level of care, and they are expected to behave rationally.[187]

2. Perverse Corporate Incentives

Scholars have considered this lack of incentives to take care ex-post as a drawback of property rules in other areas of the law where parties are affected by the interaction after the fact. For example, this is the case in environmental law for the calculations of carbon dioxide emissions.[188] When there is a lack of ex-post restrictions and monitoring, companies have incentives to take environmental risk to minimize private costs, such as those created by environment-preserving measures; costs are then externalized to the general population in the form of pollution.[189]

This moral hazard problem would further interfere with interactions between data subjects and corporations if the sole mechanism to transmit the rights over information processing were consent, as it would be under data property. Once information is collected, under a sole-consent rule the data collector has full control over the information. The uses and disclosures of the data, however, continue to affect the data subject's interests and well-being, as the Grindr case and *Frank v. Gaos* illustrate. This is because personal information inevitably retains a connection to the person even after they no longer control it.[190]

Corporations have, therefore, incentives to do two things. First, they have incentives to under-invest in care as long as they comply with external boundaries, such as cybersecurity regulations, increasing the risk of data breaches ex-post (in economists' terms, slack). For example, when encrypting, they have incentives to use minimal encryption that

187 Baker, *supra* note 178, at 277.

188 *See* Jean-Jacques Laffont, *Regulation, Moral Hazard and Insurance of Environmental Risks*, 58 J. PUB. ECON. 319, 322–24 (1995); A.P. Xepapadeas, *Environmental Policy Under Imperfect Information: Incentives and Moral Hazard*, 20 J. ENV'T ECON. & MGMT. 113, 113–15 (1991); Emmanuel Petrakis & Anastasios Xepapadeas, *Environmental Consciousness and Moral Hazard in International Agreements to Protect the Environment*, 60 J. PUB. ECON. 95, 97–103 (1996).

189 *See* Laffont, *supra* note 188, at 319–20; Xepapadeas, *supra* note 188; Petrakis & Xepapadeas, *supra* note 188.

190 Mark Verstraete, *Inseparable Uses*, 99 N.C. L. REV. 427, 466–67, 471 (2021) ("Use restrictions are necessary for governing personal data because, unlike paradigmatic commodities, personal data retains a connection to specific people that survives transfer.").

is easier to implement but also easier to override.[191] This is because the cost of any safeguards is borne by corporations, while safeguards' benefits are received by data subjects in the form of reduced risk. Thus, there is no economic reason for corporations to implement these safeguards other than compliance with regulations or a tenuous benefit over competitors from a reputation standpoint.[192]

Second, corporations have incentives to engage in high-risk activities independently of the risk that those activities create for data subjects, consequently driving up harm (in economists' terms, expropriate). For example, they have incentives to give personal data risky uses that are not in the best interest of data subjects, such as aggregating de-identified data to a point where it can be easily reidentified, or giving it away for profit, as in the Grindr example above. In the same way that the cost of safeguards is borne by corporations and the benefits accrue to data subjects—resulting in too few safeguards—the cost of further processing is borne by data subjects in the form of increased risk while the profit opportunities exist for corporations—leading to too much and too risky processing. If the benefits and costs of processing data (or enacting safeguards) were borne by the same entity, an adequate level of processing (or safeguards) could be reached. But data property cannot guarantee this.

B. *How Data Property Would Make Market Failures Worse*

1. Magnifying Existing Market Failures

A diminished version of this market failure exists in privacy statutes to the extent that they contain property rules by relying on consent at the moment of collection as a protection mechanism (a property-rule characteristic). This problem arises because property

---

191 *See, e.g.*, Leonid Bershidsky, *End-to-End Encryption Isn't as Safe as You Think*, BLOOMBERG (May 14, 2019, 7:00 PM), https://www.bloomberg.com/opinion/articles/2019-05-14/whatsapp-hack-shows-end-to-end-encryption-is-pointless [https://perma.cc/5PZQ-6RFV]; Bruce Schneier, *Why "Anonymous" Data Sometimes Isn't*, WIRED (Dec. 12, 2007, 9:00 PM), https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt [https://perma.cc/SH7H-49EP].

192 *See* Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 845 (discussing the role of reputation in corporate privacy compliance). Corporations may have incentives to provide safeguards for information only when they gain a reputation as with data subjects who would in turn react to the practice so that if corporations do not provide adequate safeguards, it would be harder for them to gain consent. In that case, the costs of inadequate security would not be entirely borne on data subjects but there would be some reputational consequences.

rules are satisfied only at the point of transfer, allowing the acquirer to ignore potential externalities later on. This can be contrasted with liability rules, which can impose costs after the transaction.[193]

The market failure would be aggravated if the law relied on data property for data subjects' protection, moving the dial further away from liability rules and into data property's exclusively-property-rule protection. If data collectors must only compensate data subjects to obtain consent to collect their personal information (for example, by providing them a service), then companies have no incentives to incur costs of care or to moderate activity levels (information processing) to avoid risk to data subjects. These are data externalities.[194]

This market failure would defeat any permutation of data property even if data subjects had perfect information, were fully rational, and could engage in capable privacy self-management—which is not the case. This is so because moral hazard does not arise from an agent failure: it arises from a combination of a party's level of risk-taking after the interaction affecting the well-being of the other and a structural lack of incentives for that party to take the other party's interest into account after the exchange. For that reason, it would be impossible for data subjects and companies to anticipate the magnitude of the moral hazard and factor it into a price for data. Prices simply cannot set adequate incentives ex-post.

Moreover, even if data subjects had full information and could calculate the expected externalities into their compensation for data, this would not solve the problem because companies would continue to lack incentives to invest in care to minimize data subject risk ex-post. If users under data property were rational, they would anticipate this increase in risk and increase the "price" demanded for their personal information in accordance with the increased risk.[195] The price increase would reduce the demand for such information in equilibrium, which would reduce the supply of information to meet that demand.[196] This moral hazard problem would, in turn, make the market unravel. This, of course, has not happened, but not because the market failure does not exist but rather because, as the last Part explained, data subjects do not make fully informed choices, so they cannot adjust for expected

193 Calabresi & Melamed, *supra* note 8, at 1110, 1119–20.

194 Schwartz, *supra* note 38, at 2084; Purtova, *supra* note 159, at 519; Spiekermann, Acquisti, Böhme & Hui, *supra* note 133, at 163; Dirk Bergemann, Alessandro Bonatti & Tan Gan, *The Economics of Social Data* (Cowles Found. Rsch. Econ., Discussion Paper No. 2203R, 2020).

195 STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 206–27 (1987) (describing insurance and the allocation of risk).

196 *See* Murphy, *supra* note 38, at 2385 (describing the "efficiency loss" associated with inhibited information disclosure due to higher cost).

risk.[197] In other words, the market does not unravel because data subjects often unknowingly make welfare-decreasing decisions.

The measures that are beneficial for data subjects, but which companies lack incentives to incorporate under a property regime, are different. These measures could be cybersecurity protections to prevent data breaches. Arguably, cybersecurity regulations mandate these protections because consent-based privacy regimes are ineffective at encouraging them. These measures could also involve avoiding risky or harmful uses of data. They could also be, for example, encouraging sufficient de-identification of data. Many activities may increase expected harm for data subjects more than they increase expected benefits for companies processing data, but companies have incentives to engage in the socially inefficient behavior because they can externalize this cost.

2. Transaction Costs in Privacy Under Moral Hazard

Economics-minded readers may wonder: if property rules are usually suggested for scenarios with low transaction costs, and the internet reduces the cost of communications (and therefore the cost of transacting, keeping all else stable), why do property rules fail to accomplish their goals in privacy?

To answer this question, one must consider that the real "cost" of someone's personal information, from that person's perspective, is not the cost of communicating the information. Rather, it is the expected harm of having their information processed, such as possibly being discriminated against, or having their information disclosed, such as having their identity stolen after a breach. The more personal information is processed, the higher the expected harm. Even absent the moral hazard market failure, for a property-rule-only system to work, data subjects would have to know the expected harm of their information in advance to ask for an equivalent price and receive compensation.[198]

Privacy harm often involves several potential parties who are unidentifiable ahead of time, many of whom only come into contact

---

197 Ignacio N. Cofone, *The Value of Privacy: Keeping the Money Where the Mouth Is*, 2015 PROC. WORKSHOP ON ECON. INFO. SEC. 1 (2015).

198 Cofone, *supra* note 157, at 524–27 (discussing "concealment and asymmetric information").

with the data ex-post.[199] Negotiating over one's information thus has high costs, even when communication costs are low. For this reason, the transaction costs of protection are more relevant than the transaction costs of communications to set a transfer rule for privacy rights.

Moreover, these transaction costs are not equally distributed. They are astronomical and unpredictable for those that are disadvantaged in society, who have fewer options and fewer means to protect themselves. This fact adds a distributional concern to the efficiency concerns of data property. Because of their lack of options, the people for whom transaction costs are higher are precisely those that, under property rules, are the least empowered to improve their situation.

In sum, unlike things that are subject to personal or real property, personal data have the capacity to affect the data subject's interest after transfer. Data property can protect from some wrongful collection, but not from wrongful use or wrongful sharing, and many of the harms related to privacy occur at these two stages. This continuity makes property rules a bad fit for personal information.

V. EXPANDING PRIVATE RIGHTS OF ACTION

Data property, as demonstrated, would create a property-rule-only regime that fails to address the moral hazard problem. Some elements that make data property undesirable are already present in American privacy law (e.g., primacy of consent, bargaining issues, companies not taking on externalities). In addition to avoiding a negative privacy law development towards data property, understanding why data property is undesirable can help improve existing and proposed privacy statutes. Dependence on property and liability rules exists on a spectrum. For any right (including privacy rights), legislators need not choose between all-property rules and all-liability rules. Since property rules are insufficient to protect individuals' personal information, liability rules must be used to address the problems presented in Parts III and IV.

Liability rules allow for ex-post compensation based on harm; and the risk of that harm depends on the corporation, not the data subject. Liability addresses moral hazard because it leads corporations to internalize such risk. Liability also compensates data subjects for the resulting harm and not just for a value negotiated or determined at the time of collection.

---

199 Amy Kapczynski, *The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism*, 59 UCLA L. REV. 970, 1009 (2012) (explaining that the cost of protecting private information "requires more than relying on formal individual consent").

These liability rules could be implemented through tort law or statutory private rights of action. Private rights of action are not a guarantee in statutory privacy, but they should be. These are absent from Virginia's CDPA.[200] Nevada's PICICA and the Colorado Privacy Act explicitly reject them.[201] They are limited in the CCPA and the California Privacy Rights Act, available only in case of a security breach.[202] And they are implemented by some, but not all, proposed state bills.[203] Broadly, liability is highly controversial in statutory privacy.[204]

A. *The Benefits of Privacy Liability*

1. Addressing Property's Problem

There is a clear benefit of incorporating liability transfer rules in privacy law to address moral hazard. Under liability rules, consent is not a prerequisite for the right's transfer. This may seem counterintuitive as a means of protection; when protected by liability rules, data subjects would be unable to block a company from using personal information. Liability rules do not aim to increase control. They aim to prevent and remedy harm when control is impossible.

Instead of "choosing" whether to allow processing and suffer future consequences, under liability rules data subjects would be compensated if any collection or processing results in harm, for

---

200 H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. §§ 59.1-571(1)–(2), 591.580(A)) (providing the attorney general the exclusive authority to enforce).

201 NEV. REV. STAT. ANN. § 603A.360(3) (LexisNexis 2017) (rejecting private rights of action); COLO. REV. STAT. §§ 6-1-1311(1) (rejecting private rights of action).

202 CAL. CIV. CODE §§ 1798.150, 1798.155 (Deering 2019).

203 They are included in the proposed New York Privacy Act, Massachusetts Information Privacy Act, and North Carolina Consumer Privacy Act, but not in the Minnesota Consumer Data Privacy Act or the Ohio Personal Privacy Act. *See* S.B. 6701, 2021–2022 Leg., Reg. Sess. § 1106.6 (N.Y. 2021) ("Any consumer who has been injured by a violation of section eleven hundred two of this article may bring an action in his or her own name."); S.B. 46, 192 Leg., Reg. Sess. (Mass. 2021); S.B. 569, 2021 Gen. Assemb., Reg Sess. (N.C. 2021). H.F. 1492, 92d Leg., Reg. Sess. (Minn. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. (Ohio 2021). Among recently proposed but now inactive bills (which nonetheless indicate how state congresses have thought about legislating privacy), they were excluded, for example, from Utah's Consumer Privacy Act and the Washington Privacy Act. *See* S.B. 200, 64th Leg., 2021 Gen. Sess. (Utah 2021); S.B. 5062, 67th Leg., 2021 Reg. Sess. §§ 101(6), 107(2), 107(4) (Wash. 2021).

204 CAMERON F. KERRY, JOHN B. MORRIS, JR., CAITLIN T. CHIN & NICOL E. TURNER LEE, BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION, Brookings Institution Report 19 (June 2020) ("No issue in the privacy debate is as polarized.").

example by causing financial damage (e.g., by identity theft),[205] reputational damage (e.g., through the dissemination of embarrassing information),[206] physical harm,[207] or discrimination.[208]

Liability rules would avoid the problems of property rules identified above. Liability rules are transactional rules that are useful when transaction costs are high.[209] And the information asymmetry between data subjects and companies operates as a transaction cost: as a consequence, data subjects face information acquisition costs that make it difficult for them to reach welfare-enhancing transactions.[210] As discussed in Part III, data subjects are likely to undervalue their data because they cannot know the magnitude of the potential risk.

Property rules' ineffectiveness due to asymmetric bargaining positions would be remedied by liability rules' ex-post compensation—which operates as collectively defined, as opposed to individually defined, "prices." Defining compensation ex-post based on harm maintains compensation for the risks that data subjects are exposed to; in contrast, defining compensation ex-ante based on bargaining would be costly and ineffective due to asymmetric information and unequal bargaining power. Indeed, the standard rationale for suggesting the use of liability rules over property rules as a transactional rule is the high cost of ex-ante bargaining.[211]

The collection, processing, and dissemination of people's personal information involve several parties, many of whom are unidentifiable ahead of time because they only come into contact with the data ex-post. Negotiating over one's information would have exorbitant transaction costs—even when the costs of surveillance and communication are low.[212] The relevant costs to determine which

---

205 *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1815 (2010); Marshall Allen, *Health Insurers Are Vacuuming up Details About You—And It Could Raise Your Rates*, PROPUBLICA (July 17, 2018, 5:00 AM), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/XG32-AXBM].

206 *See* Cofone & Robertson, *supra* note 168, at 1056–58 (arguing that privacy harm and reputational harm are conceptually distinct but are both protected by privacy rules).

207 Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655, 657–58 (2012); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 5–8 (2014).

208 *See* Ignacio N. Cofone, *Antidiscriminatory Privacy*, 72 SMU L. REV. 139 (2019) (arguing that privacy rules can be used to prevent discrimination); *see also* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

209 *See* Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027, 1036–72 (1995).

210 Litman, *supra* note 110.

211 Calabresi & Melamed, *supra* note 8, at 1110.

212 *See* Kapczynski, *supra* note 199, at 1009 (explaining that the cost of protecting private information "requires more than relying on formal individual consent").

transfer rule best protects privacy rights in each context are the transaction costs of self-protection and obtaining agreement on the transfer and the price, not the costs of surveillance or communications. In other words, even if the information and power asymmetries did not exist, the costs of bargaining over personal data would be too high because people would have to bargain with countless parties. Coupling both problems makes bargaining and control over personal information impossible.

Fixing damages in accordance with the harm caused also addresses property rules' problem of under-protecting inferred and re-identified information.[213] Aggregation, as seen above, is a problem for property rules' effectiveness: the information that is most relevant is not the disclosed information that property rules cover but aggregated information, including the inferred information made possible by such aggregation, which property rules do not cover. Under data property, data subjects would receive no compensation for harm produced by aggregated and inferred information—which is most harm. Liability rules overcome this problem because they can set compensation equal to the harm. Conversely, the expected cost of liability rules from the industry side would be equal to the expected cost of harm rather than the bargained-for price.

Due to that, moreover, an ex-post compensation would correct the moral hazard problem by varying compensation according to levels of care through liability. If data collectors' cost of processing data was not fixed ex-ante by what data subjects agreed to, but rather ex-post by the harm produced to them, the externalities introduced by moral hazard would be internalized because companies would have to take risk into account to minimize their own liability. In other words, companies would have better incentives not to overprocess data and to invest in reasonable security measures because harming data subjects would become expensive.[214] Liability rules correct moral hazard in an orthodox way: deterrence.[215]

---

213 *See generally* Ian Ayres & Eric Talley, *Distinguishing Between Consensual and Nonconsensual Advantages of Liability Rules*, 105 YALE L.J. 235, 236 n.3 (1995) (stating that, under liability rules, "even if damages are set imprecisely, liability rules can induce beneficial nonconsensual taking").

214 Contracting insurance against data breaches would, in turn, reduce the variability of the cost of harm for companies. Because insurers are in a better position to estimate risk than the average data subject, this would lead to a more accurate ex-ante premium than property rules would in the form of a price. Note, however, that the insurance market is often used as an example of a moral hazard problem.

215 *See* Robert H. Sitkoff, *The Economic Structure of Fiduciary Law*, 91 B.U. L. REV. 1039, 1042–45 (2011) ("The agent is induced to act in the best interests of the principal by the threat of after-the-fact liability for failure to have done so."); Frank H. Easterbrook & Daniel R. Fischel,

2. Accounting for Consumers' Risk Aversion

Besides addressing property rules' gaps, liability rules present an advantage regarding risk aversion. Given that, on average, data subjects are more risk-averse than corporations, liability rules would be in the interest of both players in the interaction due to their ability to hedge risk.[216] Under liability rules, not only are data subjects awarded compensation for harm but companies also face lower costs than in the impossible, hypothetical system where "perfect" bargaining can take place.

Recall *Meyers* and *Kirchein*, two cases about information collected in violation of FACTA that increased consumers' risk of identity theft.[217] What would have been adequate property-rule compensation for that information? That is, how much should each consumer have been paid to compensate them ex-ante for the risk increase? Someone could answer that the "price" should have been a monetization of the risk increase, considering both the cost of identity theft and the increase in the likelihood of an identity theft materializing as a consequence of the FACTA violation—the expected harm increase.[218] But this answer would ignore that risk itself is often harmful or inconvenient to people.[219] It is so beyond the expected monetary disutility that such risk may entail if it materializes. In other words, consumers are risk averse.[220]

If the amount of compensation is determined by the (ex-ante) expected harm, as such an answer suggests and one would expect it to be under property rules, risk aversion becomes an obstacle. People have disutility from risk that companies may not be willing to compensate. Even if a value for the data could be agreed to ex-ante (which, because

---

Corporate Control Transactions, 91 YALE L.J. 698, 702 (1982) (explaining fiduciary obligations, liability, and deterrence in corporate law).

216 *See* Calabresi & Melamed, *supra* note 8, at 1106 (explaining that risk may be reduced from a liability theory because a collective determination of value leads to quick and efficient transactions); *see also* Soo Jiuan Tan, *Strategies for Reducing Consumers' Risk Aversion in Internet Shopping*, 16 J. CONSUMER MKTG. 163 (1999) (showing in a different context that sellers' risk-reducing strategies are welfare increasing for both parties).

217 *See supra* Section III.C.

218 For example, if the probability of harm was estimated to be 10% without the FACTA breach, but is estimated to be 20% with the FACTA breach, and the harm if it happens would be $1,000, the expected harm increase would be $100.

219 KENNETH J. ARROW, *The Theory of Risk Aversion*, *in* ESSAYS IN THE THEORY OF RISK-BEARING 90, 90 (1971); John W. Pratt, *Risk Aversion in the Small and in the Large*, 32 ECONOMETRICA 122 (1964); Giora Hanoch, *Risk Aversion and Consumer Preferences*, 45 ECONOMETRICA 413 (1977).

220 *See, e.g.*, Seung Hwan Kim & Framarz Byramjee, *Effects of Risks on Online Consumers' Purchasing Behavior: Are They Risk-Averse or Risk-Taking?*, 30 J. APPLIED BUS. RSCH. 161 (2013).

of the problems above, it cannot) the value demanded by data subjects should be higher than the value offered by data collectors due to the risk averseness of the former. In other words, to adequately compensate data subjects ex-ante, companies would have to add compensation for the risk itself to the compensation for the expected harm—which they are unlikely to be willing to do. Because it avoids the disutility of risk, ex-post compensation—that is, being compensated for the harm once it happens, as opposed to being paid in advance for the expected harm whether it happens or not—is more valuable for data subjects than ex-ante compensation.[221]

Hypothetically, ex-ante compensation could take risk aversion into account and be set higher than the expected harm to account for the disutility of risk—leaving data subjects "indifferent" between ex-ante and ex-post compensation. But that permutation of property rules would be costlier than liability rules for data collectors. Even under the most expensive type of liability for companies—strict liability—liability rules' expected cost would not exceed the expected cost of harm.[222]

Because compensation should be added for the disutility of risk under property rules, any type of liability—including strict liability—is cheaper for companies than a properly executed, non-exploitative property rule. Any industry argument in favor of property rules over strict liability necessarily relies on externalities imposed on data subjects. It relies on property rules, due to the problems explored above,[223] being improperly executed.

3. Objections to Liability

The main objection to liability rules in privacy law is that privacy harm is difficult to detect and remedy.[224] Liability rules introduce

---

221 SHAVELL, *supra* note 195 at 186–205 ("In contrast to risk-neutral parties, risk-averse parties care not only about the expected value of losses, but also about the possible magnitude of losses.").

222 This conclusion would stand even with some level of overcompensation due to judicial error, as long as the overcompensation is, in expectation, lower than the amount needed to cover risk averseness.

223 *See supra* Parts III & IV.

224 Bernard Chao, *Privacy Losses as Wrongful Gain*, 106 IOWA L. REV. 555, 557 (2021) (referring to privacy harm as "by far the thorniest obstacle" to implementing liability rules); Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022) (manuscript at 29) (on file with SSRN) (stating that "[u]nder the current U.S. approach to litigation, harm plays a central gatekeeping role in many instances, and failing to recognize privacy harm shuts down important cases and prevents many privacy statutes from being effectively enforced"); Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 656 (2019)

difficulties in determining compensation—and the indeterminacy of privacy harm makes this problem more significant.[225] For example, when a website makes a ghost profile with someone's name, but the data subject lacks evidence of reputational damage, as in *Spokeo v. Robins*, courts are unsure of whether to grant them remedy.[226] Similarly, when a credit bureau is hacked but victims lack evidence that this has caused them financial damage, as in the Equifax hack, courts are unsure of whether to grant them remedy.[227]

While an in-depth exploration of this objection is carried out in a different article,[228] two things are certain. The first is that, to the extent that privacy liability does not preempt public enforcement, investigation, and FTC penalties, a lower than efficient level of liability is still an improvement over no liability at all. Believing that almost no one will sue based on privacy is a reason to be *less* worried about implementing liability, not more. The second is that, for any level of privacy harm indeterminacy, privacy harm is easier for courts and enforcement authorities to identify ex-post than it is for consumers to anticipate and prevent ex-ante.

Any objection to liability based on privacy harm indeterminacy applies, magnified, to the property-rule-only model. Moreover, there are frameworks for assessing privacy harm ex-post that courts and regulators can use.[229] But no regulator or adjudicator can anticipate this harm perfectly, much less consumers with insufficient information and no bargaining power. And the burden of anticipation adds the wrong incentives to take care ex-post when no such ex-post assessment is given.

A second objection is that relying on liability rules that depend on harm may run into problems of federal jurisdiction in terms of Article III standing according to the landmark standing case *Clapper v. Amnesty International*.[230] This case law has received a fair amount of

("Courts worry that recognizing the privacy right in the absence of a clearly defined concrete harm may lead to unpredictable, excessive damages based on plaintiffs' subjective perceptions.").

225 *See, e.g.*, Brief of the Chamber of Commerce of the United States of America, et al. as Amici Curiae in Support of Petitioner at 6–7, Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) (No. 13-1339).

226 *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).

227 *See* Editorial Board, *The Unfinished Business of the Equifax Hack*, BLOOMBERG (Jan. 29, 2019, 8:30 AM), https://www.bloomberg.com/opinion/articles/2019-01-29/equifax-hack-remains-unfinished-business [https://perma.cc/R4FW-6AAJ].

228 *See* Ignacio Cofone, *Privacy Standing*, U. ILL. L. REV. (forthcoming 2022).

229 Cofone & Robertson, *supra* note 168, at 1049–58 (presenting a model of privacy harm); Solove & Citron, *supra* note 153, at 774, 777–85 (presenting an approach for assessing risk and anxiety harms).

230 Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401–09 (2013); *see also* Bradford C. Mank, Clapper v. Amnesty International*: Two or Three Competing Philosophies of Standing Law?*, 81 TENN. L. REV. 211, 213, 255–56 (2014) (demonstrating that "[t]here has been considerable debate

criticism. Thomas Haley, for example, has argued that federal standing analysis in privacy cases harms both public policy and standing doctrine.[231] As Ari Waldman argues: "We live in a legal environment in which privacy rights mobilization is already difficult; managerial privacy compliance exacerbates the problem. Standing requirements and other hurdles hamper privacy plaintiffs' use of tort law, contract law, and federal privacy statutes to vindicate their privacy rights."[232] In an ideal world, the moral hazard problem and the consequent centrality of liability for privacy protection should lead federal courts to revise and expand standing doctrine for privacy harms.

In the meantime, state courts have enormous power to hold corporations accountable for harm. Some of the most consequential privacy cases have come from state courts. For instance, in *Rosenbach v. Six Flags*, the Illinois Supreme Court ruled that an individual need not allege an injury beyond violation of her rights under the Illinois Biometric Information Privacy Act to be considered an "aggrieved" individual.[233] The role of state courts in privacy will continue to grow as state privacy statutes introduced across the country become law. Privacy liability could function adequately while depending entirely on state courts.

B. *How to Implement Privacy Liability*

1. Liability Rules as Private Rights of Action

This Part has so far shown that, to protect privacy rights meaningfully, privacy law should include more robust liability rules in its combination of property and liability rules. The smallest change that would achieve this is keeping consent-based (i.e., property-rules-like) safeguards while enhancing the scope of private rights of action and compensable harm.

Incorporating liability rules for personal information can be achieved by creating a separate, harm-dependent private right of action

about the extent to which Congress may enlarge the definition of concrete injury under Article III" and the extent to which the separation of powers limits congressional authority to grant universal standing rights to plaintiffs who lack a concrete injury); Ass'n of Data Processing Serv. Orgs., Inc. v. Camp, 397 U.S. 150, 153 (1970) (landmark case separating the invasion of a legal interest from an injury-in-fact).

231 Thomas D. Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193 (2020); *see also* Cofone, *supra* note 228; Citron & Solove, *supra* note 224.

232 Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 812 (2020).

233 Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019).

in privacy statutes, such as the CCPA and Virginia's CDPA. Similar liability is in place for data breaches and lack of data breach notifications,[234] where plaintiffs litigate financial losses, emotional distress, costs of preventing future losses, and increased risk of future harm, among other claims.[235] Data security, indeed, is built on flexible reasonableness standards that operate ex-post,[236] which operate as liability rules. Such an approach can be expanded to privacy harm beyond data breaches.

Liability rules can also be created absent legislative reform. Courts can do so through the expansion of the privacy tort to complement statutory provisions.[237] The judiciary can achieve this by doing two things. First, by expanding the interpretation of intrusion upon seclusion and public disclosure of private facts to include harm produced by conduct that is usually in the domain of statutory regulation.[238] Second, by interpreting privacy statutes such as the CCPA and Virginia's CDPA as not preempting privacy torts.

This system would not be unique to privacy. It is common practice for administrative and tort law to be combined to prevent and compensate harm. For example, environmental law bodies sanction companies for throwing prohibited materials into a river or building with asbestos without having to prove harm because the conduct was prohibited by administrative and environmental law. Meanwhile, victims of environmental harm have a private cause of action to sue these companies for harm they have incurred.[239] State traffic law

---

234 Solove & Citron, *supra* note 153, at 739–41 ("In the past two decades, plaintiffs in hundreds of cases have sought redress for data breaches caused by inadequate data security."); William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (2019) (describing the process by which "reasonable security practices" developed).

235 Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74 (2014) (examining empirical data on data breach litigation to determine what types of data breaches are litigated more often and which are more likely to settle).

236 McGeveran, *supra* note 234, at 1195–99 (explaining how data security benefits from flexible standards).

237 *See* Citron, *supra* note 205, at 1828–52 (proposing how to expand the privacy tort and complement it with other torts to cover new ground); Bambauer, *supra* note 114, at 256–57 (discussing intrusion liability rules); *see also* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 145–56 (2007) (explaining the evolution of common law privacy). *But see* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMMS. & HIGH TECH. L. 357, 382–84 (2011) (arguing that the tort of privacy as developed by Warren, Brandeis, and Prosser is ill-equipped to address digital harms to privacy and reputation).

238 Bambauer, *supra* note 114, at 209–10, 238 (arguing that intrusion upon seclusion targets privacy concerns and that enforcement of seclusion can expand significantly).

239 Toxic Substances Control Act, 15 U.S.C. § 2641 (1986); Federal Water Pollution Control Act, 33 U.S.C. § 1319.

authorities, similarly, sanction individuals for driving with a broken light even when they did not get into an accident because of it—and one can sue when injured in an accident.[240] None of these administrative regulations preempt compensation when harm occurs.

Courts interpreting privacy statutes can similarly make room for FTC sanctions for processing personal information without justification, as stipulated by applicable statutes, while giving individuals a common law remedy to obtain compensation when harmed. Abroad, in the European Union and adequacy countries, privacy law would complement data protection authorities' sanction power in a similar way to how regulatory bodies of environmental and antitrust law are complemented in their ex-officio approach to give way for people to act.[241] Both domestically and abroad, this would complement statutes that are focused on prohibited behavior with private law lawsuits focused on harmed individuals.

In terms of legislative reform, statutes can help overcome the difficulties that courts face by (i) making an explicit choice against tort preemption and (ii) providing guidance on how privacy harm should be estimated. No privacy statutes, passed or proposed, do this yet.[242]

After determining how to approach compensation under liability rules, the next question for their implementation concerns which type of liability is the most appropriate for privacy: negligence, strict liability, or something in between (such as comparative negligence or strict liability with a negligence defense).

2. The Appropriate Standard: Negligence Versus Strict Liability

In privacy, potential tortfeasors (data collectors and data processors) are the only parties in the interaction that can exert

---

240 *See, e.g.*, Motor Vehicles and Traffic Act, GA. CODE ANN. § 40-8-20 (West 1982); N.Y. VEH. & TRAF. LAW § 375(2)(a) (McKinney 2021); WASH. REV. CODE ANN. § 46.37.040 (West 1977).

241 Michael S. Greve, *The Private Enforcement of Environmental Law*, 65 TUL. L. REV. 339 (1990) (explaining how Congress partially relies on private enforcement for public environmental law objectives); Kai Hüschelrath & Sebastian Peyer, *Public and Private Enforcement of Competition Law: A Differentiated Approach*, 36 WORLD COMPETITION 585 (2013) (explaining mixed public and private enforcement in antitrust law).

242 *See, e.g.*, CAL. CIV. CODE §§ 1798.150–17.98.155 (Deering 2019); H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. §§ 59.1-579–59.1-580); COLO. REV. STAT. §§ 6-1-1310–6-1-1312 (2021); NEV. REV. STAT. ANN. § 603A.360(3) (LexisNexis 2017); S.B. 6701, 2021–2022 Leg., Reg. Sess. (N.Y. 2021); H.B. 1602, 58th Leg., 1st Reg. Sess. § 26 (Okla. 2021); S.B. 200, 64th Leg., 2021 Gen. Sess. § 13.58.401–13.58.404 (Utah 2021); H.B. 408, 2021 Reg. Sess. § 6 (Ky. 2021); H.F. 36, 92d Sess. § 6 (Minn. 2020). Some formerly proposed bills even actively preempt privacy torts. *See, e.g.*, H.B. 216, 2021 Reg. Sess. §§ 11(a)(1), (4), 17 (Ala. 2021); S.B. 5062, 67th Leg., 2021 Reg. Sess., § 114 (Wash. 2021).

significant control over the probability of harm occurring and, if it does occur, the amount of harm.[243] This is unlike most types of accidents governed by tort law.

Liability rules aim to place the burden of care on the party who can best control the probability of the accident taking place.[244] An accident taking place depends on two things: levels of care (e.g., how attentively you drive your car) and levels of activity (e.g., how often you drive your car).

Negligence rules' comparative advantage over strict liability is that they induce an appropriate level of care from the victim and tortfeasor (but not activity), while a strict liability rule's advantage is that it induces an appropriate level of both care and activity by the tortfeasor (but not the victim).[245] While strict liability has the advantage that it can incentivize an adequate level of care and activity from the potential tortfeasor, negligence has the advantage that it can incentivize an adequate level of care by both parties—but not an adequate level of activity.[246] Tort law's deterrence tradeoff is that negligence fails at inducing appropriate levels of tortfeasor activity and strict liability fails at inducing adequate care or activity from the victim.[247] Therefore, from a deterrence perspective the question about which rule is most appropriate is a question about whether the accident is bilateral (its probability is affected by tortfeasor and victim behavior) or unilateral (its probability is affected only by tortfeasor behavior).[248]

Strict liability sets incentives for care and activity by the tortfeasor when the victim cannot affect the probability of the accident because the externality of the accident is internalized by liability.[249] If harm occurs, under strict liability the tortfeasor has an obligation to remedy the harm no matter how it took place.[250] Thus, tortfeasors are more likely to take expected harm into account under strict liability than they

---

243 *See* Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & TECH. 1, 33 (2009) (explaining that "database providers have ultimate control over use of personal information and protections that are in place").

244 Frank H. Easterbrook & Daniel R. Fischel, *Limited Liability and the Corporation*, 52 U. CHI. L. REV. 89, 102 (1985) (explaining the desirability of placing liability on the most efficient risk bearer).

245 SHAVELL, *supra* note 195, at 5–46 (introducing the theory of liability and deterrence in accident law).

246 Steven Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD. 1 (1980).

247 SHAVELL, *supra* note 195, at 73–104 (exploring factors bearing on the determination of negligence).

248 *Id.*

249 Shavell, *supra* note 246.

250 Richard A. Epstein, *A Theory of Strict Liability*, 2 J. LEGAL STUD. 151 (1973).

are under any other liability regime, in which only under certain circumstances will they be held responsible for the harm.

Such incentive-setting is relevant for resolving moral hazard. As explained in the context of product liability:

> [I]f manufacturers have more control over the safety of their products than customers [do], the insurance [that] the consumers provide to manufacturers (in the form of limited liability for products' accidents) would present a greater moral hazard than would the insurance that manufacturers provide to consumers (in the form of liability for those accidents).[251]

In technical terms, privacy harm is produced in unilateral accidents.[252] After data are disclosed, data leave the data subjects' sphere of control, thereby also rendering them unable to control the probability of harm.[253] The protection mechanisms that data subjects can use after data are disclosed have a negligible influence on the probability of data harms compared to the security measures that data processors can implement.[254]

In addition, both the level of care and the activity levels of corporations are relevant for the probability of data harm materializing.[255] The types of processing and level of database security (care level), as well as the amount of processing and number of data transfers (activity levels), affect the probability of data subjects being harmed.[256]

This is important for the choice of liability rule. The application of a negligence standard to liability for data breach notifications,[257] and for data security generally,[258] has been attacked on the basis that the correct level of due care may be uncertain, leading databases to overinvest in care. An ambiguous negligence standard would indeed introduce costly

---

251 Baker, *supra* note 178, at 280.

252 Cofone & Robertson, *supra* note 168, at 1049–53 (modeling privacy loss).

253 *See* Hoofnagle, *supra* note 243, at 1 ("One faction explains the identity theft as a problem of a lack of control over personal information.").

254 *See id.* at 34–36 (discussing internalizing externalities in the context of security measures intended to prevent identity theft).

255 *See id.* at 33 (noting that "[d]atabase operators constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database").

256 *See id.* ("The relationship is so asymmetric that the individual is literally at the mercy of the risk preferences of companies with which no relationship has even been established.").

257 Verstraete & Zarsky, *supra* note 192, at 835–37; Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. F. 614 (2018).

258 Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 261–68 (2007).

uncertainty.[259] Providing victims with compensation without having to prove corporations' negligence, as Danielle Citron explains, "would force database operators to internalize the full costs of their activities."[260] From an incentives perspective, a strict liability rule makes it easier to define expectations than does a property rule. This reflects the principle that liability rules are more efficient than property rules, even without prohibitively high transaction costs, when transaction costs stem from imperfect information.[261]

Unlike strict liability, negligence incentivizes appropriate care by the victim but, in unilateral accidents such as privacy harms, the victim's care is irrelevant. This fact makes strict liability advantageous for privacy claims. For these reasons, a strict liability rule would internalize the externalities of moral hazard and induce appropriate levels of care and activity more effectively than negligence would.

C. *Combining Public Enforcement with Private Claims*

1. Rocky Statutory Precedent for a Mixed Enforcement System

Privacy lawsuits are not new.[262] In the past, privacy problems were addressed through tort law: people sued when someone opened their letters, went through their financial papers, or disclosed harmful secrets to others.[263]

In most of statutory privacy law, however, it does not matter whether a victim was harmed, but whether a company behaved in a way

---

259 Note, however, that an ambiguous negligence standard would lead potential tortfeasors to overinvest in care only up to the investment level they would have under a strict liability rule—which would be a desirable level of care for unilateral accidents because it would fully internalize the externalities. *See* Hoofnagle, *supra* note 243, at 32–35 (suggesting strict liability for identity theft).

260 Citron, *supra* note 258, at 266.

261 *See* Ayres & Talley, *supra* note 213; Louis Kaplow & Steven Shavell, *Do Liability Rules Facilitate Bargaining? A Reply to Ayres and Talley*, 105 YALE L.J. 221 (1995); Ian Ayres & J.M. Balkin, *Legal Entitlements as Auctions: Property Rules, Liability Rules, and Beyond*, 106 YALE L.J. 703, 717–33 (1996) (describing the nonconsensual advantage of second-order liability rules); Ian Ayres & Paul M. Goldbart, *Correlated Values in the Theory of Property and Liability Rules*, 32 J. LEGAL STUD. 121 (2003) (arguing that liability rules cannot harness private information both when the disputants' valuations are correlated and when they are not).

262 *See* Solove Citron, *supra* note 153, at 781 ("Private lawsuits serve a function that these other tools lack. Such lawsuits allow individuals to have a say about which cases are brought. These lawsuits bring out facts and information about blameworthy security practices by organizations. They provide redress to victims, and they act as a deterrent.").

263 Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).

forbidden by the regulation (ex-ante).[264] This mechanism has benefits. Coupled with an enforcement authority's investigatory powers, it can produce large-scale deterrence and it can address too-dispersed externalities and harms to public goods, such as the harms to democracy seen with the Cambridge Analytica scandal.[265]

However, it is difficult to achieve compensation—together with large-scale deterrence—when fines are prioritized as an enforcement mechanism. Public regulatory enforcement by itself cannot sufficiently provide victims with compensation.

Similarly, deterrence is better achieved by a mixed system. The FTC has referred to information asymmetry, coupled with language of market failures, to promote regulatory intervention independent of data subject consent in legislative reform.[266] But both public and private enforcement are needed in practice to overcome the information and power asymmetries that exist in personal data collection, processing, and use. In other words, together with public enforcement by state attorneys general that comprehensive state statutes such as Virginia's CDPA, Nevada's PICICA, and the Colorado Privacy Act contemplate,[267] private rights of action are key for achieving citizen and consumer data protection.[268]

Other state privacy statutes give rise to private rights of action allowing for such a mixed enforcement system. Some examples are Washington D.C.'s Use of Consumer Identification Information Act,[269] and Illinois's Biometric Information Privacy Act.[270] The latter famously triggered the lawsuit against Six Flags[271] and, more recently, a class action lawsuit against Clearview AI for building one of the largest facial

---

264 *See* Janet Walker, Douez v Facebook *and Privacy Class Actions*, *in* CLASS ACTIONS IN PRIVACY LAW 56, 68–69 (Ignacio N. Cofone ed., 2020) (discussing statutory privacy in Canada); *see, e.g.*, NEV. REV. STAT. ANN. § 603A.360(3) (LexisNexis 2017) (rejecting private rights of action); COLO. REV. STAT. § 6-1-1311 (2021) (rejecting private rights of action).

265 *See* Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 105 (2019).

266 Christine S. Wilson, Comm'r, Fed. Trade Comm'n, A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Legislation 2–5 (Feb. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf [https://perma.cc/YQ6J-M4L7].

267 H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. §§ 59.1-571(1)–(2), 59.1-580(A)); NEV. REV. STAT. ANN. § 603A.360(3) (LexisNexis 2017); COLO. REV. STAT. § 6-1-1311 (2021).

268 *See* KERRY, MORRIS, JR., CHIN & TURNER LEE, *supra* note 201, at 20 (referring to joint public and private enforcement as "force multipliers"); Walker, *supra* note 264.

269 *See, e.g.*, Hancock v. Urban Outfitters, Inc., 830 F.3d 511 (D.C. Cir. 2016).

270 740 ILL. COMP. STAT. 14/20.

271 Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019).

recognition databases in history.[272] The CCPA creates civil penalties and a type of private right of action for statutory violations that gives consumers some ability to bring claims related to data security breaches (for actual or statutory damages, whichever is greater),[273] although it lacks private rights of action to enforce most of its elements.[274]

Abroad, private claims are less straightforward as they are usually based on provisions that make it difficult for individuals to bring even deserving claims successfully. For example, in Canada, starting a claim under the Personal Information Protection and Electronic Documents Act is a long process: individuals must first report it to the Office of the Privacy Commissioner, wait for the office to investigate and release a report, and then start a de novo application in court.[275]

While foreign cases based on statutory privacy are, as a consequence, infrequent, some precedent does exist. The GDPR stipulates, in this regard, space for private rights of action. Article 79 (right to an effective judicial remedy against a controller or processor) and article 82 (right to compensation and liability) contemplate the possibility of data subjects initiating actions to obtain redress, including material and immaterial harm.[276] As of today, almost all precedent on this front stems from behavior that breached the GDPR and produced material harm, with immaterial harm having virtually no traction in courts, and both material and immaterial harm without a statutory breach not being contemplated.[277] Ultimately, article 82(1) offers an ambiguous statement of claim for compensation that contributes to confusion when implemented by national courts.[278]

Reception varies by jurisdiction because the courts of Member States determine the scope and meaning of "material and non-material

---

272 Mutnick v. Clearview AI, Inc., No. 20 C 512, 2020 U.S. Dist. LEXIS 109864 (N.D. Ill. May 19, 2020) (refusing to dismiss the class action).

273 CAL. CIV. CODE §§ 1798.150, 1798.155(a)–(b) (Deering 2021).

274 Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1759 (2021).

275 *Enforcement of PIPEDA*, OFF. OF THE PRIV. COMM'R OF CAN. (Apr. 20, 2017), https://www.priv.gc.ca/biens-assets/compliance-framework/en/index [https://perma.cc/2YZC-JRBB].

276 Gabriela Zanfir-Fortuna, *Article 82. Right to Compensation and Liability*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY (Christopher Kuner, Lee A. Bygrave, Christopher Docksey & Laura Drechsler eds., 2020); *see also* GDPR *supra* note 53, at art. 82(1).

277 Eoin O'Dell, *Compensation for Non-Material Damage Pursuant to Article 82 GDPR*, CEARTA.IE (Mar. 6, 2020), http://www.cearta.ie/2020/03/compensation-for-non-material-damage-pursuant-to-article-82-gdpr/ [https://perma.cc/M32W-WCEY].

278 Eoin O'Dell, *Compensation for Breach of the General Data Protection Regulation*, 40 DUBLIN U. L.J. 97, 113–15, 147 (2017).

damages" and how much compensation is appropriate for them.[279] Traction has mainly taken place in The Netherlands,[280] Germany,[281] and Austria.[282] The United Kingdom, similarly, has seen cases in small claims courts based on article 22 of the Privacy and Electronic Communications Regulations 2003 when a corporation acts in breach of the regulation, particularly when collecting information absent a lawful basis for processing.[283]

2. Liability Must Depend on Harm

These private rights of action are the paradigmatic type of liability-rule protection over privacy rights. In a property-rule-only system, these would not exist, as it would only matter that the right is transferred with consent. However, instantiations of liability rules in current regulations are mostly limited to private rights of action for breach of the regulation, as opposed to private rights of action for the occurrence of harm. In terms of the normative considerations set above, this mechanism can be read as a liability rule with a negligence standard,

---

279 *Id.* at 115, 122 (adding that the fact that this is a state-by-state approach means that private enforcement will be uneven unless cases reach the CJEU).

280 Note that these cases have also relied on art. 6:106 of the Dutch Civil Code. *See, e.g.*, Overijssel D. Crt. (Rechtbank Overijssel), ECLI 2019 1827 (NL), https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2019:1827; Amsterdam D. Crt. (Rechtbank Amsterdam), ECLI 2019 6490 (NL), https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6490; North Holland D. Crt. (Rechtbank Noord-Nederland), ECLI 2020 247 (NL), https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNNE:2020:247.

281 *See* Jan Spittka, *Germany: First Court Decision on Claims for Immaterial Damages Under GDPR*, DLA PIPER: PRIVACY MATTERS (Dec. 12, 2018), https://blogs.dlapiper.com/privacymatters/germany-first-court-decision-on-claims-for-immaterial-damages-under-gdpr [https://perma.cc/9GXE-GDDZ]. However, other courts have disagreed. For example, German courts in 2018 and 2019 stated that a GDPR violation without material damage does not give rise to an Article 82 claim. *See* Local Court (Amtbsgericht) Diez, 2018 8 C 130/18 (DE), https://openjur.de/u/2116788.html; Karlsruhe Regional Crt. (Landgericht), 2019 8 O 26/19 (DE), https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Karlsruhe&Datum=02.08.2019&Aktenzeichen=8%20O%2026%2F19.

282 Innsbruck Higher Regional Crt. (Oberlandesgericht), 2020 1 R 182/19b (AT), at https://www.dataprotect.at/2020/03/06/post-schadenersatz. Note that the Higher Regional Court of Innsbruck reversed the judgment but not due to a disagreement in law about non-material damages but rather about the standard that should be applied for them.

283 *See* Lloyd v. Google LLC, EWCA Civ. 1599 (2019) (holding that plaintiffs may recover damages for loss of control without proving pecuniary loss); *see also* Priv. & Elec. Commc'n Regs. 2003 SI 2003 No. 2426, art. 22; Brendan Van Alsenoy, *Liability Under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 J. INTELL. PROP. INFO. TECH. & E-COM. L. 271 (2016).

where compliance with the regulation is due care that exempts from liability.

For liability to be most effective, private rights of action must be based on harm, not based on regulatory breach. This is so because of the moral hazard problem explained above. Creating a private right of action for breach of the regulation doubles down on consent and control, simply adding private enforcement. Doing so may be effective as a means of reducing public resources needed by the FTC and data protection authorities abroad, but it does not change the nature of the rules: companies can still pay attention only to the behaviors mandated and ignore whether they are producing harm. The only way to solve the moral hazard problem is to meaningfully enhance the role of liability rules in statutory privacy. And to enhance the role of liability rules is to create liability for harm created independent of whether it was a consequence of regulatory breach.

In other words, private rights of action based on harm will require companies to internalize externalities. Statutes like the CCPA that condition private rights of action on breach of regulated conduct and make them agnostic to harm do this wrongly. To be effective at protecting consumers, these private rights of action should, instead, depend on harm.

VI. BOLSTERING USE-RESTRICTIONS

As shown above, data property proposals aim to enhance something that privacy statutes have been doing all along: relying on data subjects' control for them to protect their own privacy. The difference between existing law and data property is that the latter aims to achieve that objective solely through property rules, instead of doing it by mandating and prohibiting specific activities. But control through property rules is ineffective at avoiding harm. This is a reason to strengthen ex-post accountability in privacy law.

The second way of strengthening ex-post accountability in privacy law—besides private rights of action—is bolstering use-restrictions. The single, although modest, use-restriction present in statutory privacy is the purpose limitation principle. By creating an obligation that comes after the transfer and is independent of any agreement, purpose limitation takes privacy law a step away from relying solely on property rules. The usefulness of the purpose limitation principle is illustrative of why property transfer rules applied to personal data would not work. Purpose limitation is a way to mitigate, albeit marginally, moral hazard. At the same time, the moral hazard problem

is informative of how privacy statutes should delineate purpose limitation.

A. *The Usefulness of the Purpose Limitation Principle, Revisited*

1. The Benefits of Prohibiting Purposes

Liability rules cannot solve all privacy problems. Liability cannot even solve all consent-produced privacy problems when coupled with public enforcement. Many harms are too dispersed. Some of them can be addressed through privacy class actions.[284] But how would the law internalize social externalities such as harms to democracy? It is impossible to constitute a class for social harms.[285]

Privacy law needs accountability mechanisms that address these harms. To address them, privacy law is improved by mandatory rules (provisions that cannot be waived by agreement) that set external boundaries over what corporations can and cannot do. A fraction of European-style data protection law abroad focuses on doing this: it sets mandatory rules determining what companies cannot do even after acquiring consent. For example, under the GDPR, companies cannot seek individual consent to avoid having a data protection officer, or not give explanations when the right to an explanation is triggered. These are mandatory rules that apply independent of agreements between individuals and companies. These rules exist in opposition to default rules, such as the prohibition of third-party sharing, which individuals can override by agreement, and in stark opposition to data property, under which individuals can endorse any activity.

Purpose limitation broadly construed (that is, the idea of limiting an entity's use of information for specific purposes) is an important mandatory rule because it focuses on ongoing uses. The role of this broad, conceptual purpose limitation is to limit (prohibit) certain purposes—those that are particularly risky, or not likely to be in the best interest of data subjects. A prohibition of certain purposes, while new for American privacy law, would be uncontroversial in other areas of the law. The law frequently prohibits risky uses of otherwise allowed entitlements.[286] For example, in most states, people have the right to purchase a firearm but they cannot shoot their firearm in public. This

---

284 *See* Thomas E. Kadri & Ignacio N. Cofone, *Cy Près Settlements in Privacy Class Actions*, *in* CLASS ACTIONS IN PRIVACY LAW 99, 99–112 (Ignacio N. Cofone ed., 2020).

285 Ben-Shahar, *supra* note 265, at 104–08.

286 *See generally* Hohfeld, *supra* note 61.

limits the use of firearms: to use them lawfully, people in those states must fire them in a shooting range.

One could ask based on this: do principles such as data minimization and necessity share this characteristic?[287] The answer is yes to the extent that they are mandatory rules. But they have one relevant difference in that they do not prohibit purposes. These principles reduce risk in a harm-focused manner but, because they are ex-ante, they do not address moral hazard like prohibiting purposes or setting liability rules do. Instead, these principles reduce risk by reducing companies' options.

The diluted version that exists in privacy law of that broad, hypothetical, and robust purpose limitation is the purpose limitation principle. Although it does not prohibit any particular purposes, the principle prohibits using personal data for a new purpose or collecting personal data for undeclared purposes. Because it does not limit possible purposes but it mandates their specification, it could be more accurately called purpose specification principle, as some statutes do.[288] The law should, at least, maintain and bolster this minimal limitation on ongoing use.

Incidentally, a reader could ask: if purpose limitation were to be violated, what would be the remedy? The answer is liability. A corporation that breaches purpose limitation, depending on the enforcement system, may have to pay a fine if subject to public enforcement or monetary damages if subject to a private right of action. This is where both proposals converge.[289]

2. Purpose Limitation's Standard Rationale

The purpose limitation principle is drawn from the Fair Information Practices Principles, which are the backbone of American privacy law.[290]

Purpose limitation is one of the key provisions of the CCPA, the California Privacy Rights Act, Virginia's CDPA, and the Colorado

---

287 H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. §§ 59.1-574(A)(1)–(2), 59.1-580(A)) (requiring a limit on personal data collection to what is adequate, relevant, and reasonably necessary); COLO. REV. STAT. § 6-1-1308(3) (2021) (establishing that personal data collection must be adequate, relevant, and limited to what is reasonably necessary); CAL. CIV. CODE § 1798.100(a)(3) (Deering 2019) (prohibiting the retention of personal information for longer than reasonably necessary).

288 *See, e.g.*, COLO. REV. STAT. § 6-1-1308(2) (2021).

289 In breaching purpose limitation, liability would be attributed independent of harm. It would be a liability to take a prohibited use that is risky or likely to cause harm.

290 Jones & Kaminski, *supra* note 19, at 99, 112.

Privacy Act. The CCPA adopts this principle when it requires purposes "compatible with the context in which the personal information was collected."[291] It is also included in Virginia's CDPA when it prohibits businesses from "process[ing] personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent"[292] and by the Colorado Privacy Act when it requires controllers to "specify the express purposes for which personal data are collected and processed," and prohibits "purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed."[293] But, far from being an obvious inclusion in states' privacy statutes, purpose limitation is not included in Nevada's PICICA,[294] and proposed state bills have been divided on its inclusion.[295]

Abroad, purpose limitation is a key provision of the GDPR and of privacy legislation in countries that have or seek GDPR adequacy status.[296] Purpose limitation is required by the GDPR by articles 5(1)

---

291 CAL. CIV. CODE §§ 1798.140(d), 1798.120, 1798.121(b) (Deering 2019); CAL. CIV. CODE § 1798.100(b); *see also* CAL. CIV. CODE § 1798.100(a)(1) (amending this section, effective as of 2023); CAL. CIV. CODE § 1798.100(a)(1) (containing the same provision as CCPA § 1798.100(b)), § 1798.100(c).

292 H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. §§ 59.1-574(A)(1)–(2), 59.1-580(A)).

293 COLO. REV. STAT. § 6-1-1308(2), (4) (2021).

294 NEV. REV. STAT. ANN. § 603A.360(3) (LexisNexis 2017).

295 The proposed New York Privacy Act, Massachusetts Information Privacy Act, Minnesota Consumer Data Privacy Act, North Carolina Consumer Privacy Act, and Ohio Personal Privacy Act all include purpose limitation, while Pennsylvania's bill does not. *See* S.B. 6701, 2021–2022 Leg., Reg. Sess. § 1102.1(b)(iii)(B) (N.Y. 2021) (establishing that controllers must notify consumers of "the purposes for which the categories of personal data is being shared, disclosed, transferred, or sold to the processor or third party"); *id.* § 1103.1(b)(iii)(B) (requiring that controllers delete the consumer's personal data on request where the data "is either no longer necessary to provide the services or goods requested by the consumer or for the purposes for which the consumer's freely given, specific, informed, and unambiguous opt-in consent is in effect"); S.B. 46, 192 Leg., Reg. Sess., § 6(b)(3)(ii) (Mass. 2021); H.F. 1492, 92d Leg., Reg. Sess., §§ 7(2)(a)–(c), 9(f)(1)–(3) (Minn. 2021); S.B. 569, 2021 Gen. Assemb., Reg Sess., § 75-72(a)(1)–(2) (N.C. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess., § 1355.03(E)(1)–(2)(a) (Ohio 2021); H.B. 1126, 2021 Gen Assemb., Reg. Sess. (Pa. 2021). Among recently proposed but now inactive bills, the Alabama Consumer Privacy Act, the Utah Consumer Privacy Act, and the Washington Privacy Act had included it, while the Oklahoma Computer Data Privacy Act, the Kentucky Act Relating to Consumer Privacy of Personal Information, and the previous Minnesota Consumer Data Privacy Act did not. *See* H.B. 216, 2021 Leg., Reg. Sess. (Ala. 2021) (proposed 2021); S.B. 200, 64th Leg., 2021 Gen. Sess. (Utah 2021); S.B. 5062, 67th Leg., 2021 Reg. Sess. §§ 101(6), 107(2), 107(4) (Wash. 2021); H.B. 1602, 58th Leg., 1st Reg. Sess. (Okla. 2021); H.B. 408, 2021 Reg. Sess. § 6 (Ky. 2021); H.F. 1492, 92d Leg., Reg. Sess. (Minn. 2021).

296 *See generally* Merel Elize Koning, The Purpose and Limitations of Purpose Limitation (2020) (Doctoral Thesis, Radbound University Nijmegen) (on file with Radboud University Nijmegen).

and 6(4).[297] Article 5(1)(b) establishes the need to delimit purposes anchored on a lawful basis for processing. Article 6(4) authorizes further processing for a new purpose only when compatible with the one for which the personal data was originally collected.[298] Further data processing requires a new lawful basis for it to be justified; that is, one of the legal grounds required to authorize the initial processing.[299]

These GDPR provisions are relevant to American law. The GDPR is relevant to American companies as well: since the *Schrems II* case from July 2020, they must also comply with the GDPR when collecting, processing, or distributing personal information from European data subjects.[300] The GDPR has also influenced state statutory privacy, such as the CCPA and CDPA, and will likely influence future state and federal privacy statutes.[301]

Identified purposes function as an obstacle for companies to obtain facile consent (i.e., consent that is not meaningful).[302] Data protection agencies abroad often rule that data collection was unlawful because data subjects were unaware of the purpose for which their data were being collected. For example, in 2011 the Canadian Office of the Privacy Commissioner found that a complainant was uninformed concerning the collection of her personal information because its purpose was vague—and therefore she did not meaningfully consent.[303] In 2014, it asked an organization to translate its policy because the complainant was uninformed concerning the collection purpose due to her limited

---

297 Jones & Kaminski, *supra* note 19, at 108, 112–15.

298 *See* GDPR, *supra* note 53, at art. 6(4)(a)–(e).

299 Judith Rauhofer, *"Look to Yourselves, That We Lose Not Those Things Which We Have Wrought." What Do the Proposed Changes to the Purpose Limitation Principle Mean for Public Bodies' Rights to Access Third-Party Data?*, 28 INT'L REV. L. COMPUTS. & TECH. 144 (2014).

300 *See* Data Prot. Comm'r v. Facebook Ir. Ltd [2020] C-311/18 (H. Ct.) (Ir.) (invalidating the Privacy Shield program that exempted U.S. companies from complying with GDPR by allowing them to comply instead with a special U.S.–E.U. hybrid system).

301 *See* Hartzog & Richards, *supra* note 133, at 1711–13 (discussing the GDPR and CCPA in relation to principles for fair information processing).

302 *See* European Commission Press Release 17/EN, The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Article 29 Data Protection Working Party, *Guidelines on Consent Under Regulation 2016/679*, EUROPEAN COMM'N (Nov. 28, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [https://perma.cc/YZA5-YMSV]; OFF. OF THE PRIV. COMM'R OF CAN., CONSENT AND PRIVACY: A DISCUSSION PAPER EXPLORING POTENTIAL ENHANCEMENTS TO CONSENT UNDER THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* (2016), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605 [https://perma.cc/W78P-U7CF].

303 *Public Opinion Research Firm Must Better Inform Survey Respondents About Their Personal Information Use; Refrain from Collecting Full Birth Dates*, OFF. OF THE PRIV. COMM'R OF CAN. (Sept. 4, 2013), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-011 [https://perma.cc/2C2V-NE43].

understanding of English.[304] By doing so, the principle reduces the asymmetric information and unequal bargaining power problems.

3. Purpose Limitation and Property Rules

The irony is that property rules in personal data are incompatible with a wide application of the purpose limitation principle. Property rules operate based on the transferability of the rights they protect,[305] making it more difficult to impose any restrictions ex-post.[306] Cohen pointed to this idea when arguing that property is incompatible with privacy because property is "grounded in a theory of self-actualization based on exchange—designed to minimize transaction costs and other obstacles to would-be traders, and thus systematically, inevitably biased toward facilitating trade in personally-identified information."[307]

Notably, property rules allow for subsequent sales once information is acquired—as with any physical object that one can re-sell after buying.[308] In this way, while property rules may appear consumer-protective, they lower transaction costs for subsequent sales, making risky third-party sharing easier for companies.[309]

Property rules keep transaction costs relatively low precisely because consent (to transfer a right) needs to be acquired once, and not again for reusing or reselling the entitlement that was transferred through consent.[310] The purpose limitation principle removes this characteristic. The purpose limitation principle does so because it restricts what can be done with the information after a transfer, meaning that the company acquiring the information cannot use it or

---

304 *Investigation into the Personal Information Handling Practices of Ganz Inc.*, OFF. OF THE PRIV. COMM'R OF CAN. (Oct. 7, 2014), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-011 [https://perma.cc/ET38-YQH4].

305 Samuelson, *supra* note 82, at 1138–39 (using the language of property rights and identifying free alienation as a problem of property).

306 Schwartz, *supra* note 38, at 2090.

307 Cohen, *supra* note 10, at 1375.

308 Peter P. Swire, *Markets, Self-regulation, and Government Enforcement in the Protection of Personal Information, in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997) (arguing that if such sales are made illegal, it would not stop the sales from occurring, but merely cause sales to be more expensive).

309 Cofone, *supra* note 157, at 543–44 (discussing the "non-collection default rule").

310 *Id.* at 545 ("If companies had to ask Internet users for permission each time such information was traded, transaction costs would be too high."). Note that, however, if there is consent for a transaction different than transferring the right, such as a license in copyright, then consent would have to be reacquired for anything that exceeds what was agreed on, such as the scope of the license.

share it with another party without a new agreement to do so.[311] Requiring companies to ask data subjects for permission each time such information was traded keeps transaction costs higher than with property rules.[312]

By removing the property-rule characteristic of acquiring consent only once, the purpose limitation principle reduces moral hazard in two ways. The first way is that it reduces the information asymmetry between consumers and companies. Moral hazard arises partly because of such information asymmetries.[313] By increasing transparency about the uses that can be given to information, a source of uncertainty is removed because the levels of ex-post risk are partly determined by new, risky uses. This method is orthodox for addressing moral hazard in consumer law, as is done through warranties, which reduce uncertainty about products' durability.[314]

The second way is that it generates ex-post accountability. Such ex-post accountability reduces moral hazard between companies and consumers because it places ongoing use restrictions on personal data. The purpose limitation principle does not eliminate moral hazard, as companies can still use and share personal data in risky ways without internalizing such risk. But the scope of possibilities becomes more limited. Reducing the scope of behavior from the more-informed party, as the purpose limitation principle does, is a way to reduce moral hazard in economics.[315]

Ultimately, specifying purposes in advance mitigates the problems identified above, even if it does not solve them entirely. Because purpose limitation is a well-tried principle already embedded in American law, it is a low-cost intervention that can, at least in part, mitigate the moral hazard problem.

---

311 Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1006 (2017); David Basin, Søren Debois & Thomas Hildebrandt, *On Purpose and by Necessity: Compliance Under the GDPR*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 20, 23 (Sarah Meiklejohn & Kazue Sako eds., 2018).

312 Swire, *supra* note 308 (stressing the importance of keeping overall prices low).

313 Holmström, *supra* note 183, at 74 (showing that improving on imperfect information can reduce the moral hazard problem in principal-agent relationships).

314 Nancy A. Lutz, *Warranties as Signals Under Consumer Moral Hazard*, 20 RAND J. ECON. 239, 240–45 (1989) (presenting a model of warranty provision).

315 Patrick W. Schmitz, *Allocating Control in Agency Problems with Limited Liability and Sequential Hidden Actions*, 36 RAND J. ECON. 318, 221–25 (2005) (discussing sequential agency problems' optimal organization).

B. *Property and Liability in Purpose Limitation*

1. (Limited) Lessons from Intellectual Property

This last point relates to the difference between ownership rights and property rules explained above. While, in ownership over real or personal property, rights are often transferred in their entirety—meaning that the new owner can do with it what she desires[316]—this is not the case for all other ownership-similar types of rights. Ownership-similar rights, such as intellectual property rights, are protected by a mix of property and liability rules.[317]

Take the example of copyright. Regarding the property characteristics of copyright law, authors holding copyright are entitled to exclude others from copying their work.[318] The holders can either transfer copyright in its entirety or (more frequently) grant a license for the use of their work in exchange for a royalty,[319] partially alienating their rights to exclude and to request injunctions for the breach of such exclusion.[320]

Regarding copyright's liability characteristics, authors face some compulsory licenses and must accept fair use.[321] While compulsory licenses tend to be specific and limited, fair use is a central trait of copyright law.[322] Purpose limitation, which allows for ongoing use-restrictions as opposed to permanent transfers, finds analogs in copyright law.

Like other liability rules, fair use is justified by high transaction costs. Specifically, by the high transaction costs that would otherwise be

---

316 However, not all tangible property transfers are in fee simple (although most chattel transfers are). For example, one can grant a limited easement for a neighbor's passage over part of one's land without transferring ownership; one can grant a time or activity-limited license for entry to one's land while making anyone who exceeds that license a trespasser; and one can make a conditional transfer such that the new owner forfeits her rights if she violates the condition.

317 *See* BJ Ard, *More Property Rules than Property? The Right to Exclude in Patent and Copyright*, 68 EMORY L.J. 685, 697–99 (2019) (describing the liability rule features of copyright).

318 *See id.*

319 *See* WILLIAM CORNISH, DAVID LLEWELYN & TANYA APLIN, INTELLECTUAL PROPERTY: PATENTS, COPYRIGHT, TRADEMARKS AND ALLIED RIGHTS 525–30 (8th ed. 2013).

320 *See* Ard, *supra* note 317, at 712–14 (arguing that copyright statutory damages awards are often high enough to function as property rules).

321 Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217, 233.

322 *See* 17 U.S.C. § 107 (2012); *see also* Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1110–25 (1990) (discussing fair use's contours); Glynn S. Lunney, *Fair Use and Market Failure: Sony Revisited*, 82 B.U. L. REV. 975, 979–96 (2002) (discussing fair use in the context of a copyright dispute).

incurred in negotiating and monitoring the uses that it protects.[323] For example, the law allows quoting scientific works without the author's permission arguably because obtaining such permission every time would create exceedingly high transaction costs, while citations do not harm the author's economic interest.[324] If the quotation is large enough to cover and thereby substitute for the whole work, on the other hand, it would harm the author's economic interest, and the law requires permission to do so.[325]

Compulsory licenses, similarly, are a liability rule designed to facilitate non-consensual use of an entitlement: them being compulsory means that the right-holder has no choice over the transfer.[326] Compulsory licenses are often set at actual damages (or an estimate of how the entitlement would be priced in a market transaction), which allows for their use as long as it is efficient for users to pay that collectively determined price.[327] Compulsory licenses under copyright law are analogous to the purpose limitation principle. Both specify the objective for which the information can be used and forbid its use for other purposes.

An argument can be made in favor of liability rules in privacy law based on this similarity.[328] This is not to say that privacy law should be part of or further resemble intellectual property law. This has been shown to be incompatible due to the different aims of intellectual property law and privacy law.[329] What the analogy does, rather, is show that some of the most protective features of privacy law, such as the

323 Wendy J. Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and Its Predecessors*, 82 COLUM. L. REV. 1600 (1982).

324 In expectation, they do not reduce the expected number of copies sold—they may even increase sales.

325 In general, fair use finds its scope defined in the uses of the product that do not significantly affect the economic interests of the owner and, as a doctrine, strives to prevent the stifling of creation. *See* Leo J. Raskind, *A Functional Interpretation of Fair Use: The Fourteenth Donald C. Brace Memorial Lecture*, 31 J. COPYRIGHT SOC'Y 601 (1983); Richard A. Posner, *When Is Parody Fair Use?*, 21 J. LEGAL STUD. 67 (1992).

326 *See* Christopher M. Newman, *A License Is Not a "Contract Not to Sue": Disentangling Property and Contract in the Law of Copyright Licenses*, 98 IOWA L. REV. 1101 (2013).

327 *Id.*

328 On the other hand, use restrictions in the form of non-compulsory licenses are compatible with property-rule protection (e.g., a licensee can only obtain rights barred by the license through bargaining, a licensee who exceeds the license's terms is subject to injunctive relief rather than compensatory damages, and a non-licensee who tries to engage in the licensed activity is also subject to injunctive relief).

329 Samuelson, *supra* note 82, at 1140–41; Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 5, 8; *see also* Ritter & Mayer, *supra* note 45, at 222 (proposing property rights while acknowledging that "these enormous data sets have nothing to do with the creative artistic assets that copyright laws serve to protect").

purpose limitation principle, are not based on property rules and, moreover, are incompatible with enhancing the role of property rules.[330] The intellectual property analogy can illustrate, in other words, why it is undesirable to be concerned exclusively with information's initial transfer, like data property advocates are.

2. Purpose Limitation's Liability and Market Failures

Because of its liability rule characteristic of operating ex-post, the purpose limitation principle mitigates the problems of asymmetric information, unequal bargaining positions, and unprotected inferred data. The prohibition on asking consumers to agree to the use of data for any purpose is a limit on contractual freedom that mitigates the unequal bargaining positions problem. It marginally reduces asymmetric information because it establishes that companies will not use the data for unknown purposes. It reduces the problem of inferred data because it poses limits on corporations' ability to create more inferred data.

An example of purpose limitation being used for these aims exists in the GDPR. GDPR purpose limitation prohibits bundling consent, which is a way for corporations to abuse bargaining power and information asymmetry.[331] Since inferences constitute a new purpose, purpose limitation is a useful tool to prevent the unexpected aggregation of information into new information about consumers without their knowledge.[332]

Here a reader might wonder: Seeking authorizations from data subjects for each secondary use of information would increase transaction costs, especially given that personal information is valuable when aggregated—and that processing involves many data subjects. Is the purpose limitation principle not, then, a property rule, to the extent that it enhances exclusion? Fair use means that one can use someone else's copyrighted work without their consent, but purpose limitation

---

330 Samuelson, *supra* note 82, at 1155–56 ("Trade secrecy law has a number of default rules that might be useful for information privacy protection. The general rule of trade secrecy licensing law is that if the licensor has provided data to another for a particular purpose, the data cannot be used for other purposes without obtaining permission for the new uses. . . . One of the most significant advantages of the licensing regime is that it avoids the problems of a property rights approach . . . .").

331 GDPR, *supra* 53, at art. 7(4), Recital 32, 43; ARTICLE 29 WORKING PARTY, GUIDELINES ON CONSENT UNDER REGULATION 2016/679, at 5–7 (2018).

332 *See* Nikolaus Forgó, Stefanie Hänold & Benjamin Schütze, *The Principle of Purpose Limitation and Big Data*, *in* NEW TECHNOLOGY, BIG DATA AND THE LAW 17, 17 (Marcelo Corrales, Mark Fenwick & Nikolaus Forgó eds., 2017).

means that to use someone else's personal information one needs *further* consent. Why is this further consent not property-rule-compatible?

The difference lies in who holds the right. In fair use, for example, the author holds the copyright-created right. Using it without acquiring consent is replacing a property rule with a liability rule. In purpose limitation, after having collected information under a lawful basis (and potentially compensating the data subject) under property rules the corporation would hold the right and could therefore do with the right as it sees fit. The purpose limitation principle shows that not all privacy rights are transferred by data subject consent, as they would be under data property, because data subjects retain rights over that information. Data property would eliminate such protections.

C. *Purpose Limitation Reform*

1. Purpose Specificity

Based on what was argued above about the importance of the purpose limitation principle and how it interacts with property and liability rules in privacy, law reform proposals can be developed to make the purpose limitation principle more effective at addressing moral hazard.

First, legislative reforms could require that the stated purpose must be specific.[333] This is the case under the GDPR.[334] As Hoofnagle explains, "vague and abstract purposes such as 'promoting consumer satisfaction,' 'product development' or 'optimizing services' are prohibited."[335] But several other jurisdictions allow for vague purposes.[336] The proposal to incorporate this requirement may carry

---

333 Joseph A. Cannataci & Jeanne Pia Mifsud Bonnici, *The End of the Purpose-Specification Principle in Data Protection?*, 24 INT'L REV. L. COMPUTS. & TECH. 101, 102 (2010) ("[W]atering down 'purpose' . . . is an indication that the bigger picture (or human dignity and *lex personalitatis*) is being ignored or worse eroded.").

334 Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, EUROPEAN COMM'N (Apr. 2, 2013), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [https://perma.cc/4PYP-RW86]; Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 77 (2019) (discussing the purpose limitation principle).

335 Hoofnagle, van der Sloot & Borgesius, *supra* note 334, at 77 ("A specific purpose exists, for example, when a pizza delivery service asks for the consumer's address, to deliver the pizza.").

336 *See, e.g.*, Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5, § 4.2.2 (Can.).

extra weight for countries seeking to acquire or maintain GDPR adequacy status.

In jurisdictions that lack this specificity requirement, identified purposes not found in breach of this provision and considered sufficiently limited have included statements as broad as "workforce productivity" or "market research."[337] Those purpose formulations can be helpful for organizations, but not for data subjects. A reframing of purpose limitation with the objective of informing data subjects about the aims of the data collection, processing, and dissemination would better mitigate the asymmetric information and bargaining power problems.

This change could be implemented through statutory reform in proposed bills by adding the specificity requirement in purpose limitation provisions, but it can also be implemented without law reform. The CCPA, the California Privacy Rights Act, the Colorado Privacy Act, and Virginia's CDPA all include the purpose limitation principle broadly (without explicitly requiring specificity).[338] The specificity requirement could be implemented by the enforcement authorities, such as state attorneys general, that must interpret the statute when enforcing it. These authorities could (and should) take the opposite route of authorities abroad that have accepted wide purposes like "workforce productivity" and "market research."

2. Clear Standard

A second recommendation is for enforcement authorities to develop a standard for assessing when use or dissemination constitutes a new purpose. Such a standard would, in turn, determine when use or dissemination must be communicated to the data subject with a new request for consent.[339] This standard can be created by legislators engaged in statutory reform or by enforcement authorities.

---

337 *See, e.g.*, *Use of Personal Information Collected by Global Positioning System Considered*, OFF. OF THE PRIV. COMM'R OF CAN. (Nov. 30, 2006), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-351 [https://perma.cc/XD3L-9KB8] (finding acceptable the purpose of "managing workforce productivity"). *See generally* MAXIMILIAN VON GRAFENSTEIN, THE PRINCIPLE OF PURPOSE LIMITATION IN DATA PROTECTION LAWS (2018).

338 CCPA 1798.100(b); CAL. CIV. CODE §§ 1798.100(a)(1) (containing the same provision as CCPA 1798.100(b)), 17.98.100(c) (Deering 2019); COLO. REV. STAT. § 6-1-1308(2), (4); H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. § 59.1-574(A)(1)–(2)).

339 Rauhofer, *supra* note 299, at 146–47 (discussing different interpretations of purpose limitation's compatibility rule).

One way to conceive such a standard is by implementing a reasonableness standard.[340] It would ask: "did the data subject have a reasonable expectation that consent would be re-acquired for the subsequent use or dissemination?" A reasonableness standard for purpose limitation would stand in contrast to private law standards in most other technical contexts, such as standards in professional responsibility.[341] The explanation is that this standard would primarily aim to reduce the information asymmetries that magnify moral hazard, rather than to increase verifiability for facilitating the determination of liability, as professional responsibility standards do.

This standard would fit under the principle in privacy law of considering people's reasonable expectations of privacy.[342] Although one could fear that technical aspects would be a poor fit for this reasonableness standard, the standard would be compatible with a data-subject-focused purpose limitation principle that aims to reduce moral hazard. A reasonable person standard would be closer than a technical standard to the idea that the purpose should be specified to data subjects in understandable terms.[343]

If enforcement authorities care about reducing moral hazard, in other words, they have good reasons to mandate purposes to be specified in writing for data subjects, not for regulators, so as to increase certainty and foreseeability.

---

340 *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, OXFORD BUS. L. BLOG (Oct. 28, 2020), https://www.law.ox.ac.uk/business-law-blog/blog/2020/10/duty-loyalty-privacy-law [https://perma.cc/GA7B-UBC3] (developing an ex-post accountability mechanism consisting of a heightened reasonable person standard through a duty of loyalty).

341 *See* Clark C. Havighurst, *Altering the Applicable Standard of Care*, 49 L. & CONTEMP. PROBS. 265, 266 (1986) ("The impossibility of precisely articulating in advance the performance required of a health care provider under all possible circumstances explains why professional custom has been widely used as a benchmark for evaluating a professional's work. Indeed, if there is to be accountability at all, any specification of the obligation of true professionals to their clients must at some point have reference to what other professionals would do under the same circumstances."); Jane P. Mallor, *Liability Without Fault for Professional Services: Toward a New Standard of Professional Accountability*, 9 SETON HALL L. REV, 474, 477–79 (1978) (discussing the policy principles relating to standards in professional responsibility).

342 *See, e.g.*, GDPR, *supra* note 53, at Recital 50 (stating that people's "reasonable expectations" will be considered); *see also* S.B. 6701, 2021–2022 Leg., Reg. Sess. § 1102 (N.Y. 2021).

343 *See* Hoofnagle, Van der Sloot & Borgesius, *supra* note 334, at 77 ("[T]o assess whether a new purpose is compatible with the original purpose, the controller should consider, for instance, the link between the original and new purposes, the context, the data subject's reasonable expectations, the data's nature and sensitivity, the consequences of the intended further processing for data subjects."); *see also* GDPR, *supra* note 53, at art. 5(1)(a), Recital 39.

3. Prohibited Purposes

The third recommendation that stems from the failings of data property is to include prohibited purposes. This is a more significant deviation from current law. Until this point, this Part argued for implementing the purpose limitation principle in proposed bills by requiring that specific purposes are disclosed at the moment of data collection. As mentioned, specifying purposes is the smallest possible intervention that is helpful for mitigating the moral hazard problem. Prohibiting purposes that are considered particularly risky is a more ambitious permutation of the same principle.

Prohibited purposes are the missing element of purpose limitation that can maximize its potential for creating ex-post accountability. Included under the broad idea of purpose limitation, this measure would identify specific uses for personal data as too risky. Instead of having individuals (or the market) decide which purposes are acceptable, these purposes would be identified through the political process. It can thus be seen as a collective, rather than individual, purpose limitation.

Beyond purpose limitation, data protection law abroad sometimes desirably engages in more substantive ongoing use-restrictions by prohibiting certain uses or purposes that may be highly risky for data subjects. A recent example of this—although technically outside data protection law—is the proposed European Union's A.I. Act.[344] The Act is structured by risk, prohibiting some uses of AI that are considered the riskiest, such as social scoring in the public sector and facial recognition for law enforcement with exceptions.[345] Interestingly, the Act includes a harm requirement in the prohibitions, stating that it is for an activity within the specified parameters that "causes or is likely to cause that person or another person physical or psychological harm."[346] Such probabilistic harm requirement (while it could be criticized for limiting the provision's scope) is illustrative of the link between ongoing-use restrictions and liability rules because it makes explicit that such ongoing-use restrictions are designed not to maximize control but to prevent harm.

The advantage of incorporating prohibited purposes is that doing so frees data subjects from having to self-manage purpose-related

---

344 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 [https://perma.cc/T89Q-98E8].

345 *Id.*, tit. II, art. 5.

346 *Id.*, art. 5(b).

choices, on which they continue to have asymmetric information and unequal bargaining power. It avoids placing the burden on data subjects to make risk-reducing choices at the moment of data collection.

In the language discussed here, such a reform of the purpose limitation principle would take it further away from property rule protection (dependent on consent) and towards liability rule protection (dependent on collective mechanisms).[347] Private rights of action, moreover, are fully compatible with such a mechanism. Individuals could still seek redress individually; they would just do so for actions that were determined to be wrong by the political process, not the market.

CONCLUSION

Data property proposals are widely misunderstood, aim at the wrong goal, and would be self-defeating if implemented. Policy, media, and academic proposals to protect privacy with property abound. These proposals do not aim to create ownership rights over data; rather, they propose protecting existing privacy rights with what Calabresi and Melamed call property rules.

In other words, data property proposals do not propose mutating the content of privacy rights but rather ensuring that these rights are transferred solely by consent and in exchange for an agreed-upon price. The first portion of this Article is thus corrective: when people argue for "property over data," they are arguing for "some kind of right over data, not necessarily a property right, that is protected by a property rule." This means that, to refute the proposal (as typically stated) that "people should have property over data," one's target should be the claim that "people should have some kind of right over data, protected solely by property rules."

These property rules produce problems specific to privacy. The second portion of this Article shows the flaws in data property that make it inadequate at protecting privacy rights. Data property proposals leave out important dignitary considerations, ignore asymmetric information and unequal bargaining power, and fail to address the harms produced by aggregated and inferred personal data. These problems indicate that data property bolsters the wrong protection mechanism.

But data property has an additional problem that defeats its own goal of guaranteeing individual control. Privacy harm can be produced

347 *See* Calabresi & Melamed, *supra* note 8, at 1110.

at the moment of collection, processing, or dissemination of personal information. And property rules can only control the moment of collection. By condensing protection guarantees to the moment of collection (in property terms, exchange for a price), property rules produce a moral hazard problem: unless otherwise constrained,[348] companies lack incentives to minimize processing and disclosure harms after the exchange has taken place. This means that data property not only has the wrong goal (control), but also fails to achieve that goal.

This finding does more than provide a normative reason not to implement data property. It also provides insights for privacy law reform. Statutory privacy reforms should complement their property rule elements with liability rules. This Article explores two ways to do this. The first is allowing for private rights of action. For them to reduce the moral hazard problem, private rights of action must be orthogonal to the basis for collection and depend on the creation of harm, irrespective of how such harm occurred. The second is reinforcing use-restrictions, particularly the purpose limitation principle. While purpose limitation improves consent, it ironically contradicts property rules by placing limitations on use and disclosure after the exchange.

Without statutory reform, both proposals can be advanced by courts. Regarding the first, there is value in interpreting privacy statutes as (i) including liability rules and (ii) not preempting tort law claims, thus using tort law as a complement to statutory privacy. Regarding the second, courts could interpret the specificity of purposes more narrowly than they currently do, ruling that too-broad purposes (such as "marketing purposes") breach purpose limitation. So could enforcement authorities such as state attorneys general and the FTC.

Legislators and enforcement authorities should abandon the idea that property solves control problems in privacy law. Instead, they should underpin accountability mechanisms for privacy harm. All in all, it is crucial for privacy law to focus on what happens beyond the point of transfer, which is the only point that data property scrutinizes.

---

348 *See, e.g.*, COLO. REV. STAT. § 6-1-1308(5) (establishing the duty to take reasonable measures to secure personal data from unauthorized acquisition during storage and use); H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at VA. CODE ANN. § 59.1-574(A)(3)) (including the obligation to establish, implement, and maintain reasonable data security practices); CAL. CIV. CODE § 1798.100(e) (Deering 2019) (establishing the obligation of reasonable security procedures and practices).