BEYOND DATA OWNERSHIP

Ignacio Cofone*

43 Cardozo L. Rev. __ (forthcoming 2021)

ABSTRACT

Data ownership proposals 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: a moral hazard problem where corporations lack incentives to reduce privacy harm. That 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 discussion on how to formulate federal and state privacy statutes. These

---

* Assistant Professor and Norton Rose Fulbright Faculty Scholar, McGill University Faculty of Law. ignacio.cofone@mcgill.ca. Many thanks to BJ Ard, Michael Beauvais, Elettra Bietti, Rebecca Crootof, Christopher Essert, Inge Graef, Nikolas Guggenberger, Tom Haley, Claudia Haupt, Chris Howard, Martin Husovec, Shaz Jameson, Anthony Niblett, Przemyslaw Palka, Alicia Solow-Niederman, Adriana Robertson, Teresa Scassa, Mark Verstraete, Jacob Victor, and Ari Waldman for their helpful comments. The 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 an academic visit at the Tilburg Institute for Law, Technology, & Society was supported by Microsoft and financial support for research assistance was provided by the Social Sciences and Humanities Research Council. I also thank Ana Qarri, Jeremy Wiener, Vanessa Di Feo, and Martina Kneifel for their fantastic research assistance. I'm grateful that the Article received the Council of Europe Stefano Rodota Award Special Jury Mention.

involve implementing a combination of what the Calabresi-Melamed framework calls property and liability rules. This mixed rule system is essential because property rules alone fail to protect data subjects from the risks of future uses and abuses of their personal information. The Article implements this reform proposal with two recommendations. First, it proposes bolstering private rights of action for privacy harm irrespective of whether such harm was coupled with a statutory breach. Second, it proposes reinforcing ongoing use restrictions over personal data by strengthening the purpose limitation principle, a key and underutilized ongoing use restriction in American law.

TABLE OF CONTENTS

I. INTRODUCTION

The idea that privacy should entail ownership over one's personal data has rapidly gained popularity in recent 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] This Article engages with data ownership in three ways. First, it revisits and improves popular understanding of data ownership proposals. Second, it identifies a problem that makes these proposals self-defeating. Third, it develops, on the basis of such critique, proposals for privacy law reform.

---

[1] *See*, *e.g.*, Own Your Own Data Act, S. 806, 116th U.S. Congress (introduced March 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), www.forbes.com/sites/angelauyeung/2019/02/14/california-wants-to-copy-alaska-and-pay-people-a-data-dividend--is-it-realistic.

[2] *See infra* Part II.A.

[3] *See infra* Part II.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 209–233 (2018) (including in the proposal both personal and non-personal information).

[6] Ben Dickson, *How Blockchain Solves the Complicated Data-Ownership Problem*, THE NEXT WEB (Aug. 17, 2017), thenextweb.com/contributors/2017/08/17/blockchain-solves-complicated-data-ownership-problem/ ("Blockchain Technology provides an alternative that gives the ownership of data back to users.")

Data ownership proposals contain a conceptual ambiguity that has created a blind spot in both the arguments in their favor and valid criticisms against them. Despite the language that proponents use,[7] data ownership proposals have not proposed creating ownership rights over data.

Ownership rights (i.e., property rights) is a closed-form bundle of *in rem* rights. But data ownership proposals do not suggest implementing this type of rights over data. Instead, these proposals aim to maximize data subject control over their personal information by reinforcing consent and, consequently, creating a marketplace for data. Such a market is supposed to extract larger ex-ante compensation for users.

The proposals rely on property *rules* and not property *rights*, which are consequentially different. Property rules stipulate that a right can only be given away with consent.[8] The mainstream discourse on data ownership argues that data should be transferred solely by property rules—even if some proponents may believe that they are applying property rights. One can see this from the language used in the proposals, the absence of ownership rights' key elements, and the emphasis they 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 by a property rule*.[9] This Article is the first to clarify this conceptual ambiguity. The Article thus refers to these proposals as "data property."

This Article's clarification shows that data property is subject to criticism on new grounds. Prior scholarship has shown how 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 excavates two sets of problems that have so far not been identified.

---

[7] *See infra* Part II.

[8] Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1089 (1971).

[9] *See infra* Part III.B.

[10] *See*, *e.g.*, Julie Cohen, *Examined lives: Informational privacy and the subject as object*, 52 STAN. L. REV. 1373, 1408–16 (2000). *See also infra* Part III.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 meaningfully improve data subjects' vulnerable situation.

Second, understanding data property as transfer rules allows one to see how data property is counterproductive for 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 the data transaction. Therefore, they generate a moral hazard problem: companies have incentives to engage in risky uses and disclosures of data ex-post. This reduces people's long-term control over their personal data and exposes them to more harm. This moral hazard problem makes data property self-defeating.[16]

This critique informs privacy law discussions that do not overtly use the language of property but nevertheless share some of data property's elements by relying on consent. The failures of data property show that having ex-post accountability in addition to consent-based rules is a necessary condition for a robust protection of people's privacy. Privacy law must protect privacy rights with both consent-based rules (which

---

[11] *See* Václav Janeček, *Ownership of Personal Data in the Internet of Things,* 34 COMP. L. & SEC. REV. 1039, 1041 (2018). *See also infra* Part III.

[12] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882–83 (2012); Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV 431, 444 (2017) (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, 130–152, 165–72 (2013). *See also infra* Part IV.A.

[14] *See* Neil M. Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 Yale L.J. 1180, 1184 (2017). *See also infra* Part IV.B.

[15] *See* Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471,1475, 1489–1490 (2018). *See also infra* Part IV.C.

[16] *See infra* Part V.B.

operate before-the-fact) and accountability mechanisms (which operate after-the-fact). The Article explores two ways to do this. Privacy law reforms must (i) combine consent requirements with new private rights of action and (ii) keep and reinforce restrictions on the use of personal data.

The first normative proposal involves establishing private rights of action to enforce privacy.[17] Personal information needs liability rules because these rules respond to the market reality by not relying on unequal bargaining between consumers and companies and by encompassing inferred data. They address the moral hazard problem by forcing companies to internalize the expected cost of their data use and sharing. Because of these functions, liability rules can address property rules' deficiencies in protecting privacy.

The second normative 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 be given different uses later on. 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, and it remains unclear whether an eventual federal privacy statute would.

These normative proposals are particularly relevant now, as sates continue to formulate their own privacy statutes and the federal government considers a (possibly preemptive) federal privacy statute.[20] Virginia's Consumer Data Protection Act (CDPA), for example, includes purpose limitation but not private rights of action,[21] while some proposed

---

[17] *See infra* Part VI.
[18] *See infra* Part VII.
[19] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENVER L. REV. 93, 99–112 (2020).
[20] Thomas Germain, *State Privacy Laws Move Forward, but Are they Strong Enough?*, CONSUMER REPORTS (Feb. 23, 2021) (reporting that 2021 is the busiest year for state privacy legislation in history); Jennifer Bryant, *2021 Best Chance for US Privacy Legislation*, IAPP PRIVACY ADVISOR (Dec. 7, 2020) (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) (discussing the possibility of a federal privacy statute).
[21] Consumer Data Protection Act, H.B. 2307, 2021 Sp. Sess. §§ 59.1-574(1), (2) (Va. 2021), lis.virginia.gov/cgi-bin/legp604.exe?ses=212&typ=bil&val=hb2307.

state acts do the reverse.[22] The Article's proposals can also be implemented within current statutes. The first proposal can be used by courts when ruling over standing for privacy harms. The second proposal can be used by the Federal Trade Commission in interpreting the scope of purpose limitation.

The Article proceeds as follows. The next Part provides an overview of the data property proposals in legislation, the media, private industry, and academia. Part III 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 IV outlines how existing criticisms of privacy law apply to data property once interpreted correctly. Part V explains why data property would introduce an additional, fatal flaw that would lead it to defeat itself: a moral hazard problem. Parts VI and VII propose two directions for regulations to move past the ameliorated version of the moral hazard problem that exists in privacy law. Part VI explains how statutes can develop a combination of property with liability rules by creating harm-dependent private rights of action. Part VII suggests reinforcing the purpose limitation principle to better ex-post accountability.

II. THE POPULARITY OF DATA OWNERSHIP

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.

---

[22] Oklahoma Computer Data Privacy Act, H.B. 1602 (2021).

Legislation is a good example of this trend. Senator John Kennedy for example, introduced in 2019 the Own Your Own Data Act, which 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 rely on property over data.[24] Former presidential candidate (and current candidate for New York City mayor) Andrew Yang has been explicit in his proposal that personal data should be treated as a property right, 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 called *Humanity Forward* that advocates for "data as a property right."[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

---

[23] Own Your Own Data Act, S. 806, 116th U.S. Congress (introduced March 14, 2019).

[24] Jill Cowan, *How Much Is Your Data Worth?* N.Y. TIMES (Mar. 25, 2019), www.nytimes.com/2019/03/25/us/newsom-hertzberg-data-dividend.html (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), www.forbes.com/sites/martyswant/2019/10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/.

[26] Samuel Haig, *Mt. Gox CEO Slams Plaintiff for Adjusting Fraud Allegations Mid-Case*, COINTELEGRAPH (Mar. 17, 2020), cointelegraph.com/news/mt-gox-ceo-slams-plaintiff-for-adjusting-fraud-allegations-mid-case; Andrew Yang, *Regulating Technology Firms in the 21st Century*, YANG2020 - ANDREW YANG FOR PRESIDENT, www.yang2020.com/blog/regulating-technology-firms-in-the-21st-century/. *See also Andrew Yang Explains Why Digital Data Is Personal Property | NBC News Now*, NBC NEWS (Oct. 14, 2019), www.youtube.com/watch?v=tSOf0Eh-4dU. *See also* Jaron Lanier & E. Glen Weyl, *A Blueprint for a Better Digital Society*, HARV. BUS. REV. (Sept. 26, 2018), hbr.org/2018/09/a-blueprint-for-a-better-digital-society (presenting the idea of "data dignity" and arguing that data is a form of labour and taking it without compensation is labour exploitation).

[27] HUMANITY FORWARD, movehumanityforward.com/; Tyler Sonnemaker, *Andrew Yang wants you to make money off your data by making it your personal property*, BUS. INSIDER (Nov. 14, 2019), www.businessinsider.com/andrew-yang-data-ownership-property-right-policy-2019-11.

information.[28] More hesitantly, in 2017 the European Commission launched a consultation group assessing data ownership,[29] and regulating data ownership is part of the coalition treaty of the German ruling parties.[30]

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] Also in 2018, writer Evgeny Morozov argued in *The Guardian* that big tech should consider abandoning targeted advertising and move to an ownership-based subscription system with monthly charges.[32] *The Economist* published in 2019 that people must own their personal data as a matter of human rights, arguing that "data itself should be treated like property and people should be fairly compensated for it."[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

---

[28] Standing Committee on Access to Information, Privacy & Ethics, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, HOUSE OF COMMONS CANADA (June 2018), www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf.

[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*, EUROPEAN COMMISSION (July 2, 2014), www.eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0442&from=EN.

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

[31] Editorial, *Digital Privacy Rights Require Data Ownership*, FIN. TIMES (Mar. 3, 2018), www.ft.com/content/a00ecf9e-2d03-11e8-a34a-7e7563b0b0f4.

[32] Evgeny Morozov, *After the Facebook Scandal, It's Time to Base the Digital Economy on Public v. Private Ownership of Data*, THE GUARDIAN (Apr. 1, 2018), www.theguardian.com/technology/2018/mar/31/big-data-lie-exposed-simply-blaming-facebook-wont-fix-reclaim-private-information.

[33] *We Need to Own our Data as a Human Right—and Be Compensated for It*, THE ECONOMIST (Jan. 21, 2019), www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it.

[34] Robert Shapira & Siddhartha Aneja, *Who Owns Americans' Personal Information and What is it Worth?*, FUTURE MAJORITY (Mar. 8, 2019), assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf.

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]

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]

---

[35] *Why You Should Own Your Data*, SEGMENT, segment.com/academy/intro/why-you-should-own-your-data/.

[36] Benoit van Abroeck, Julien Debussche & Jasmien Cesar, *Building the European Data Economy – Data Ownership White paper*, BIRD & BIRD 121 (Jan. 1, 2017), sites-twobirds.vuture.net/1/773/uploads/white-paper-ownership-of-data-(final).pdf (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), www.investopedia.com/news/blockchain-could-make-you-owner-data-privacy-selling-purchase-history/ ("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."); Steven Perry, *Who Owns the Blockchain*, IMB DEVELOPER (May 7, 2018), developer.ibm.com/code/2018/05/07/who-owns-the-blockchain/ ("Whether the blockchain is anonymous (public blockchain) or private (permissioned blockchain), the nature of ownership is fundamentally the same: shared…"); 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), bdtechtalks.com/2017/06/01/whats-the-value-of-blockchain-to-consumers/ ("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), medium.com/@markvanrijmenam/how-blockchain-will-give-consumers-ownership-of-their-data ("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 (1995); Corien Prins, *When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter*, 3 SCRIPTED 270 (2006) ("With the growing economic importance of services based on the processing of personal data, it is

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]

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

---

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. 2056, 2076–2094 (2003) (proposing a property-style approach to regulating personal information).

[39] Kenneth Laudon, *Markets and Privacy*, 39 COMM. ASSOC. COMP. 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 42; Lawrence Lessig, *The Architecture of Privacy*, 1 VANDERBILT J. ENTERTAINMENT L. & PRACTICE 56 (1999); 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); 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. TELECOMM. & TECH. L. 367, 380–84 (2012) (focusing on health privacy); Jim Harper, *Perspectives on Property Rights in Data*, AMERICAN ENTERPRISE INST. (Aug. 8, 2019), www.aei.org/technology-and-innovation/perspectives-on-property-rights-in-data/.

[40] *See* Prins, *supra* note 42, 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. RES. 247 (2002) (adding that arguing that it would "allow individuals to differently value their privacy" at 261).

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] 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.[44]

In one of its most recent permutations, data property exists under the pay-for-privacy movement.[45] 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.[46] While building on property, these proposals contain a slight deviation from usual conceptions of private ordering in mandating of 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 data as labor for companies that acquire such data.[47] Data used by

---

[42] Jeroen van den Hoven et al., *Privacy and Information Technology*, STAN. ENCYCLOPEDIA PHIL., plato.stanford.edu/archives/win2019/entries/it-privacy/ (last updated Oct. 30, 2019).

[43] Leon Trakman, Robert Walters and Bruno Zeller, *Is Privacy and Personal Data Set to Become the New Intellectual Property?*, 50 INT'L REV. INTELL. PROP. & COMPETITION L. 937, 951 (2019) (adding that "a constrained conception of IP rights can assist in reconciling principles of contract and general property." at 952). *See also* Will Rinehart, *The Law & Economics of "Owning Your Data"*, AMERICAN ACTION FORUM (Apr. 10, 2019), www.americanactionforum.org/insight/law-economics-owning-data/.

[44] Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 221, 260–76 (2016) (discussing the particulars that regard implementing their proposal).

[45] *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), time.com/5230506/facebook-pay-ad-free/.

[46] Elvy, *supra* note 4, at 1400-28 (2017) (showing that pay for privacy models turn privacy into a tradeable product).

[47] POSNER & WEYL, *supra* note 5, at 209–233 (including in the proposal both personal and non-personal information).

companies is produced by humans who are not on their payroll, including their proposal personal data, for example during the use of websites or apps, and non-personally-identifiable data, for example when completing a captcha.[48] In Weil's words, "data as lab or treats them [personal data] as user possessions that should primarily benefit their owners."[49] Separately, Weil has argued with Jaron Lanier that, because data is a form of labor, it is labor exploitation to take it without compensation.[50]

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."[51] Canadian businessman Jim Balsillie, similarly, has argued in Parliament that, due to the effects of the European Union General Data Protection Regulation (GDPR),[52] people have personal ownership of their data, and such data ownership must be woven into a national data strategy.[53] These appear frequently from overheard conversations on the bus to Reddit.[54]

---

[48] *Id.* at 209–233.

[49] Imanol Arrieta-Ibarra et al., *Should We Treat Data as Labor? Moving beyond "Free"*, 108 AEA PAPERS AND PROC. 38, 40 (2018).

[50] Jaron Lanier & E. Glen Weyl, *A Blueprint for a Better Digital Society*, HARV. BUS. REV. (Sept. 26, 2018), hbr.org/2018/09/a-blueprint-for-a-better-digital-society (proposing the establishment of "mediators of personal data", which operate similarly to data trusts, and tying it to the idea of data dignity).

[51] Jennifer Barker, *Vestager on the intersection of data and competition*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Oct. 3, 2018),

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) [hereinafter GDPR].

[53] *Evidence from the Standing Committee on Access to Information, Privacy and Ethics*, HOUSE OF COMMONS CANADA (May 10, 2018), www.ourcommons.ca/Content/Committee/421/ETHI/Evidence/EV9861805/ETHIEV106-E.PDF.

[54] *See*, *e.g.*, *This Guy is Selling all his Facebook Data on eBay*, REDDIT (May 29, 2018), www.reddit.com/r/technology/comments/8n2s04/this_guy_is_selling_all_his_facebook_data_on_ebay/ ("You do own it. And in exchange for using Facebook's

These blanket descriptive statements that privacy law grants property over personal data are incorrect.[55] In Teresa Scassa's words "the control provided under data protection laws falls short of ownership."[56]

However, privacy law does contain some property-like elements.[57] Data property proposals involve moving the dial further towards them. While this Article is concerned with *normative* data property proposals, the descriptive statements show that, because of the property elements in current privacy law, data property critiques inform privacy law discussions.

III. WHAT DATA PROPERTY REALLY MEANS

As the reader 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.

---

services you give them the right to sell it." [user: jmlinden7]); "Why is it so bad that my data is being sold or stolen by mega corporations?", REDDIT (Feb. 2, 2013), www.reddit.com/r/NoStupidQuestions/comments/8gnzx0/reddit_why_is_it_so_bad_that_my_data_is_being/ ("Why is someone else earning money off your data and not you ?" [user: DisRuptive1]); *My "Own Your Data" Data Project*, REDDIT (July 8, 2014), www.reddit.com/r/selfhosted/comments/b6o8lu/my_own_your_data_project/.

[55] Nadezda 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 (2011).

[56] Teresa Scassa, *Data Ownership*, CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION, Report No. 187, 13 (Sept. 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).

[57] *See* Jacob M. Victor*, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, Note,* 123 YALE L.J. 513, 515 (2013) ("The Regulation takes the unprecedented step of, in effect, creating a property regime in personal data, under which the property entitlement belongs to the data subject… The Regulation's use of property-derived rights is particularly unusual"); Thomas 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).

A. Rights and transfer rules

The key role of privacy law is to establish rights (entitlements) and their corresponding obligations over personal information.[58] But together with establishing rights, the law regulates their transfer.[59] Establishing a right and establishing its transactional structure are independent operations.[60] This transactional structure determines under which conditions valid exchanges (transactions) over those rights happen.

The law establishes this structure by placing transfer rules over rights.[61] There are three types of transfer rules: property rules, liability rules, and inalienability rules.[62] Rights protected by a property rule are transferred with the title-holder's consent and in exchange for a price determined through bargaining.[63] Examples of these are everyday contracts. Rights protected by a liability rule are transferred without the title-holder's consent and in exchange for a judicially determined price.[64] Liability rules are used mainly due to high transaction costs of ex-ante bargaining—or an actual impossibility.[65] For example, if a factory pollutes in breach of environmental law, they 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.[66] For example, an

---

[58] 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* [add Hohfeld cite] (discussing jural correlatives).

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

[60] *Id.* at 1090.

[61] *Id.*

[62] Calabresi & Melamed, *supra* note 33, at 1092 (noting that these types are not "absolutely distinct").

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

[64] *See*, *e.g.*, *Id.* at 1107–10 (identifying eminent domain as an example of liability rules).

[65] *See Id.* at 1110 ("efficiency is not the sole ground for employing liability rules rather than property rules").

[66] *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").

agreement to sell an organ will be rendered void.[67] Property rules, liability rules, and inalienability rules thus define the transactional structure of the rights they protect, whichever those rights are.[68]

Ownership—which is confusingly 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.[69] 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.[70]

Ownership right (or a property right) is a type of right that can be protected by any transfer rule: a property rule, a liability rule, or an inalienability rule.[71] In contrast—in an unfortunate ambiguity—property rules are a transfer rule based on consent that can be used for any type of right.[72]

For example, being compensated after a car crash is a liability rule over an ownership right over one's car, as eminent domain is a liability rule over an ownership right over one's land. Buying the car or 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 a liability rule for damage to something (one's body parts) that cannot be described as ownership.

---

[67] 42 U.S.C § 274e.
[68] Klevorick, *supra* note 57, at 907 (discussing this in the context of criminal law).
[69] Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics Essay*, 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 systems"). *See also* James E. Penner, *The Bundle of Rights Picture of Property*, 43 UCLA L. Rev. 711, 739–767 (1995) (discussing the bundle of rights view).
[70] *See* Lisa Austin, *The Public Nature of Private Property*, *in* PROPERTY THEORY: LEGAL AND POLITICAL PERSPECTIVES (James Penner & Michael Otsuka eds., 2018).
[71] Calabresi & Melamed, *supra* note 8.
[72] Calabresi & Melamed, *supra* note 8.

Subletting a room in an apartment is a property rule over something one does not own. Similarly, transferring 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 right they have to occur via property rules.

		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 privacy rights. While inalienability rules are uncommon and their justifications vary,[73] the law frequently alternates between property and liability rules.[74] If one protects privacy through property rules, the right-holder (data subject) will have the right to decide who can access and use her personal information and who cannot, hence excluding others from accessing the information. If privacy interests are protected by liability rules, the right holder will have a right to be compensated whenever someone breaches her right by accessing or using her personal information in a harmful way.

Consent follows property rules. Broadly speaking, "understood as a crucial mechanism for ensuring privacy, informed consent is a natural corollary of the idea that privacy means control over the information about

---

[73] 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 J. Radin, *Market-inalienability*, 100 HARV. L. REV. 1849, 1903–1936 (1987) (evaluating market-inalienability); Lee Anne Fennell, *Adjusting Alienability*, 122 HARV. L. REV. 1403 (2009).

[74] Rose-Ackerman, *supra* note 70, at 937–41 (providing efficiency and equity arguments for one transfer rule over another); Radin, *supra* note 70; Fennell, *supra* note 42.

oneself."[75] 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.

Placing property rules (due to the ambiguity I explain below, sometimes misconceptualized as ownership) over personal information has been defended on the grounds that it would force a negotiation that would alter this.[76] 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).[77] Data subjects, moreover, would be able to extract ex-ante compensation for its release,[78] and they would receive compensation for the expected privacy cost associated with each information disclosure.[79] While this initially *sounds* desirable, there are several 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 treat it as a type of right, but as a transfer rule.

Recall that a property right (ownership) is a type of right that can be regulated by any transfer rule.[80] Property-rule protection of personal information amounts to a non-collection default that applies unless

---

[75] 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, and Helen Nissenbaum eds., 2014).

[76] *See* LESSIG, *supra* note 43 at 85–90; LAWRENCE LESSIG, CODE 2.0 200-33 (2006).

[77] Laudon, *supra* note 43; Murphy, *supra* note 42; Lessig, *supra* note 43; Mell, *supra* note 43; LESSIG, *supra* note 43, at 85–90.

[78] *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1092 (1999) ("Property rules involve a collective decision as to who is to be given an initial entitlement but not as to the value of the entitlement.").

[79] *See* Prins, *supra* note 42 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.").

[80] *See supra* Part III.A.

consent is given.[81] Property rights often (but not always) have a transactional structure established by property rules. Sometimes, property rights are 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.

Arguing that personal data should be a property right could take either of two forms: arguing that it should have the same bundle of *in rem* rights as ownership rights do, or arguing that it should have the main characteristic of ownership: the *in rem* right to exclude others from the thing over which one has property.[82] 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.[83] This is not what data property proposals suggest.

Proposals in favor of treating privacy as property emphasize consent as the valve to authorize giving away privacy. 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—that a bundle of rights akin to conventional property should be assembled to replace privacy rights. They instead suggest that the rights that data subjects hold over their personal information (privacy rights) should not be transmitted without their consent and for a socially established compensation, but rather with their consent and for a bargained-for compensation. Transfer by consent, however, is not unique of property rights.

---

[81] *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").

[82] *See* Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 734–740 (1998) (canvassing perspectives on the right to exclude).

[83] Václav Janeček, *Ownership of Personal Data in the Internet of Things,* 34 COMP. L. & SEC. REV. 1039, 1041 (2018) (comparing civil and common law and stating that "civilian idea of ownerships as an absolute dominion encompassing all the listed rights over the relevant subject; whereas in the common law tradition, ownership includes a variety of different rights over the same property"). *See also* PURTOVA, *supra* note 40.

Some of the proposals described in the previous Part are examples of this. The report to the Canadian House of Commons, for example, focuses on doing away with non-consented collection and use of citizens' personal information.[84] Yang's proposals, similarly, focus on allowing individuals to "share in the economic value generated by their data,"[85] when the way compensation is allocated 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;"[86] and control depends on the mechanism through which rights are transferred, namely property transfer rules. 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 be ownership rights err in that, without specifying the transfer rule, this identification does not arrive at the kind of protection that they seek.

This even extends to most proposals that have used the language of privacy as ownership, which have used property and ownership indistinctly. Most academic and policy discussions of data property do not mean a property right. They mean property rules. This is because, like those suggesting data as property, they 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. For example, van den Hoven explores ownership as a means of maximizing

---

[84] Standing Committee on Access to Information, Privacy and Ethics, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, HOUSE OF COMMONS CANADA (June 2018), www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf.

[85] Yang, *supra* note 25.

[86] *See* Mark van Rijmenam, *How Blockchain Will Give Consumers Ownership of their Data*, MEDIUM (July 5, 2019), markvanrijmenam.medium.com/how-blockchain-will-give-consumers-ownership-of-their-data-3e90020107e6. *See also* Dickson, *supra* note 35 ("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.").

data subjects' control over their personal information,[87] even though the type of entitlement does little to enhance the right-holder's control over it—it is the transfer rules which do.

Some scholars have hinted at this mischaracterization. Julie Cohen's critiques described below, for example, apply to property rules. Teresa Scassa, similarly, has said that "Although the personal data economy is burgeoning, it appears to be based more on contractual models than on any underlying ownership right in personal information."[88] But the mischaracterization, which is enormously consequential for how one should address these popular proposals and how one should address elements of property in privacy law, has remained underexplored.

The exclusionist conception of property rights, because it focuses on the ability to exclude (and exclusion must be done through an assertion, which is similar to the opposite of consent),[89] rings similar to the property transfer rules. This may indeed be the 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 this Article showed, 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, which is conceptualized as a separate right of the bundle.[90] 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 proposal argues 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 to prevent people at the supermarket from noticing I bought a can of tomato soup, but I retain a right under both on whether

---

[87] Van den Hoven et al., *supra* note 46 at 3–4 (referring to the concept of "self-sovereign identity").

[88] Scassa, *supra* note 41, 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")..

[89] Merrill and Smith, *supra* note 66, at 360–66 (defending the exclusionist view).

[90] JOHN G. SPRANKLING, UNDERSTANDING PROPERTY LAW 4–5 (2d ed. 2007) (noting that the right to exclude and right to transfer are difference sticks in the bundle).

the store owner can enter the information into a customer data bank to then sell to third parties. My right is not *in rem* because it does not accompany the information.

In addition, there is an important conceptual difference: 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 less important for physical objects, where use and transfer are dissociated clearly: I can lend my soccer ball while retaining my right to exclude you from it. With information, transfer and use get muddled:[91] letting Google use my personal information strikes very 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 the property rule for transfer is more important than it is for physical objects, as it is needed to prevent abuses.

Property rules are one version of transfer rules. Realizing this is enormously consequential. Identifying the correct transfer rules is key for privacy law because privacy is about appropriate information flows.[92]

In sum, when people have referred to property over data, they most of the times have meant data protected by a property rule, 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's protected by a property rule*.

As the next two Parts explain, this view is objectionable on different grounds. Scholars have correctly argued that the property conception faces important limits. But viewing the property conception for what it is allows one to see that it also defeats itself.

---

[91] Helen Nissenbaum, *Must Privacy Give Way to Use Regulation?*, in DIGITAL MEDIA AND DEMORATIC FUTURES 255, 264–69 (Delli Carpini ed., 2019), https://nissenbaum.tech.cornell.edu/papers/Digital%20Media%20and%20Democratic%20Futures_Chapter10.pdf (indicating that the distinction between data collection and use has fuzzy boundaries and leads to slippery slopes).

[92] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 131–36 (2004).

C. Inadequate goal

Data property, which seeks to promote data subjects' control over personal information, has been criticized for pursuing the wrong goal.[93] This is because privacy is about more than individual control. As Lisa Austin argues, not even Alan Westin, often read as the paradigmatic defender of privacy as control, supports a narrow, control-only definition of privacy.[94]

Ultimately, privacy is necessary for protecting individuals' autonomy. A lack of privacy can lead an individual to feel that she is under surveillance or scrutiny by others.[95] As a result, her spectrum of thoughts and behaviors may be tailored to those that she perceives others consider acceptable, thereby limiting her freedom to develop as an autonomous person.[96] This leads privacy to be a central part of reflective citizenship.[97] Privacy, thus, is much more than individual control.

Respecting privacy is crucial for valuing individuals.[98] Elettra Bietti, for example, has argued 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."[99] For that reason, she argues that shaping the data economy through transfer and acquisitions is reductive.[100]

---

[93] *See*, *e.g.*, Cohen, *supra* note 10, at 1377.
[94] Lisa M. Austin, *Re-reading Westin*, 20 THEORETICAL INQUIRIES IN L. 53, 58–63 (2019) (discussing how Westin also understands privacy in terms of a condition's experience).
[95] *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).
[96] Stanley Benn, *Privacy, Freedom and Respect for Persons*, *in* PRIVACY: NOMOS XIII 8 (Ronald Pennock & John Chapman eds., 1971).
[97] 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).
[98] Ari E. Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69:3 U. MIAMI L. REV. 559, 582–85 (2015) (linking this idea to sociology).
[99] Elettra Bietti, *Locked-in Data Production: User Dignity and Capture in the Platform Economy* 19* (forthcoming 2021), http://dx.doi.org/10.2139/ssrn.3469819
[100] *Id.*

Julie Cohen famously argued that property cannot support a broad conception of the protection of privacy.[101] 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."[102] 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.[103] But unlike other market goods, personal information is part of people's person.[104] Relatedly, data property has been said to raise constitutional issues, particularly in terms of speech.[105]

Equating data with tradability is precisely what property rules—but not property rights—do. Thus because Cohen's critique focuses on the problems of tradability, it effectively problematizes the application of property rules to personal data. As I showed above, this is what data property proposals do. Her critiques therefore apply to data property proposals (as I reframed them), and not merely to the strawman of creating ownership rights over personal data. Cohen shows, in other words, that data property proposals pursue an inadequate goal.

IV. WHY THE PROPERTY CONCEPTION IS INEFFECTIVE: OLD REASONS APPLIED TO NEW GROUND

Once one understands data property for what it is—protecting privacy through consent and independently of harm—one can see that a number of criticisms that have been made to other aspects of privacy law problematize data property. Because of its focus on trade, data property creates three structural problems in the protection of privacy rights. First,

---

[101] Cohen, *supra* note 10, at 1380.

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

[103] Cohen, *supra* note 10, at 1384.

[104] *Id.* at 1378 ("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").

[105] 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 issue. Facts are basic buildings blocks: building blocks of expression; of self-government; and of knowledge itself.").

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 obtained through data aggregation. These structural problems are discussed in the next three subsections, respectively.

A. Asymmetric Information

The last Part showed that data property is not concerned with the type of right but rather with transferring it through consent.[106] For that reason, the limits of the notice and choice paradigm also translate into the data property. Although this Article is not about the benefits and limits of consent in privacy, notice and choice's asymmetric information problem is relevant because it transfers into data property.[107]

Solon Barocas and Helen Nissenbaum have said that "big data extinguishes what little hope remains for the notice and choice regime."[108] While many call for more companies to implement consumer privacy notices as a way to increase transparency,[109] others suggest that notices

---

[106] *See supra* Part III.B.

[107] *See, e.g.*, Elena Gonzalez & Paul De Hert, *Understanding The Legal Provisions That Allow Processing And Profiling Of Personal Data—An Analysis Of GDPR Provisions And Principles*, 19 ERA FORUM 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.)

[108] Solon Barocas & Helen Nissenbaum, *Computing Ethics Big Data's End Run Around Procedural Privacy Protections*, 57:11 COMM. 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" at 31). *See also* Strandburg, *supra* note 15, 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).

[109] Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1047–59 (2011) (proposing visceral notices for privacy); Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory System*, 34 FLA. STATE UNIV. 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 Health Care*, 99 COLUM. L. REV. 1701, 1715–20 (1999) (explaining the provision of notices as a common method for regulation in medicine).

are ineffective at increasing consumer awareness of how their personal information is managed, even if they are simplified and even if people read them.[110] Indeed, empirical evidence has shown that simplifying disclosures has no effect on consumer awareness, suggesting that language complexity is not the main driver.[111] 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.[112]

This limitation on the usefulness of notices may be due to information overload.[113] That is, it may be the case that the reason why notices are rarely effective is that, no matter how simple of a formulation they have or how 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?). [114] 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.[115]

---

[110] 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. 191, 204–06 (2016) (using a vignette study to show that formal privacy notices actually reduce consumer trust on a website). *See also* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, PROCEEDINGS OF THE ENGAGING DATA FORUM (2009); Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. L. POL'Y INF. SOC. 543, 544 (2008) (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 BAYL. 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).

[111] Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. LEGAL STUD. 41, 44 (2016) (finding that best-practice simplification techniques have little or no effect on respondents' comprehension of disclosures).

[112] Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. 69, 76–83 (2016) (testing language in privacy policies).

[113] Ignacio N. Cofone, *A Field Experiment on Biased Beliefs and Information Overload in Consumer Privacy* (draft 2021, on file with author).

[114] *Id.*

[115] Ari E. Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 113 (2018) (characterizing design's effect as "powerful"); Ari E. Waldman, *A Statistical Analysis of Privacy Policy Design*, 93 NOTRE DAME L. REV. ONLINE 159, 163–171 (2018) (discussing a survey's findings).

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.[116] 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).[117] And digital consent rarely meets these conditions.[118]

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.[119] From a 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"[120]). 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 individuals.[121]

---

[116] *See infra* Part IV.C.
[117] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent* 96 WASH. L. REV. 1461, 1476–91 (2019).
[118] *Id.* at 1498–1502.
[119] *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 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).
[120] Lisa M. Austin, *Enough About Me: Why Privacy is About Power, Not Consent (or Harm), in* A WORLD WITHOUT PRIVACY?: WHAT CAN/SHOULD LAW DO 8 (Austin Sarat ed., 2014).
[121] *Id.*

Because data property pivots on consent and control, the asymmetric information criticism of the notice and choice system extends to the reliance on consent by property rules.[122]

B. Unequal bargaining positions

A limitation of data property is that it assumes that data subjects are able to manage risks in their ability to consent. That will rarely be the case.

Due to the type of interactions in which privacy policies are involved, where data subjects have a take-it-or-leave-it option, it is at least questionable to believe that reinforcing property rules would improve data subjects' bargaining position.[123] Under property rules, data subjects frequently face a take-it-or-leave-it option between using the product and giving their personal information for free, or not using the product at all.[124] If they need to use the service, for example, because it is part of normal social life and therefore costly to opt-out of such as email or a cellphone provider, this consent would then not be given freely.[125]

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.[126] 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

---

[122] *See* Richards & Hartzog, *supra* note 14, at 444 (explaining that the narrative of control feeds from the narrative of privacy self-management). *See also* Neil M. Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 Yale L.J. 1180, 1184 (2017).

[123] Sarah Spiekermann et al., *The Challenges of Personal Data Markets and Privacy*, 25 ELECTRONIC MARKETS 161, 166–67 (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).

[124] *See* Samuelson, *supra* note 75, at 1162 (describing the contractual elements of this relationship).

[125] Bietti, *supra* note 95, at 29* ("The problem, also, is that opting 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").

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

their personal data.[127] This model fails to address the unequal bargaining positions between data subjects and information intermediaries as well as the data aggregation problem explained below.

There is, at a broader level, an information asymmetry problem between data subjects and data processors that makes consumers vulnerable.[128] Data subjects lack technical knowledge necessary to sufficiently understand terms and conditions.[129] Moreover, understanding them, let along bargaining over them, would take an enormous amount of time.[130] It is difficult to believe, in this context, even with the existing efforts on reinforcing meaningful consent, that data subjects would make informed and welfare-enhancing decisions.[131]

In addition, it is impossible for data subjects to properly assess the risks involved in disclosing their personal information in the current environment.[132] Data subjects cannot assess the risks of disclosing because

---

[127] *Id.* at 1883 (noting that privacy 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).

[128] Schwartz, *supra* note 42, at 2076. Tony Vila, Rachel Greenstadt and David Molnar, *Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market*, PROC. OF THE 5TH INT'L CONF. ON ELECTRONIC COM. (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 (2012) ("A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched").

[129] Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES IN 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).

[130] McDonald & Cranor, *supra* note 107, at 544.

[131] *See* Strandburg, *supra* note 15, at 95 ("In a functioning market, payment of a given price signals consumer demand for particular good 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).

[132] *Id.* at 19 ("it 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 75, at 1128, 1145 (noting that commentators think the law should supply corrective measures).

they do not always know how their data *will* be used and what *can* be done with it.[133] Some also argue that data processors even have economic incentives to mislead data subjects, which adds to the problem.[134] "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."[135] This information asymmetry has been used in the United States to justify regulatory intervention independent of data subject consent in legislative reform with the explicit language of market failures.[136] The costs of assessing risks when providing consent are therefore high.[137]

C. Data aggregation

Another problem is that information is routinely assembled through data aggregation; that is, by compiling different types of information provided by the data subject, perhaps to different companies, at different times. This information is inevitably 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 no obstacles to how freely consent is given, the data subject would receive ex-ante compensation only for providing consent for each piece of information released to each data collector.

---

[133] Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471,1475, 1489–1490 (2018) (discussing information overload and aggregation).

[134] Trakman, Walters and Zeller, *supra* note 47.

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

[136] Christine S. Wilson, *A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation* (*Remarks at the Future of Privacy Forum*), U.S. FED. TRADE COMM. (Feb. 6, 2020), ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf.

[137] Samuelson, *supra* note 75 (adding that while most objects that are sold can be replaced, one cannot replace personal data once it is disclosed).

However, she would not have ex-ante compensation for the aggregated information, which is more valuable and potentially more harmful.[138]

Taken individually, these data might not even be valuable enough to induce companies and data subjects to bargain over them but,[139] combined, they present high costs to users.[140] And the way that information aggregates, as well as how high these costs are, are extremely difficult for data subjects to estimate.[141] 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.[142]

Another extension is that much personal information, and therefore one's lack of privacy, is inferred not only from information that one releases but also from information provided by or taken from others.[143] Data about different people are frequently combined.[144] That has led some

---

[138] Barocas & Nissenbaum, *supra* note 72, at 32 (discussing the harm aggregated information poses); Solove, *supra* note 12, at 1889–991; Strandburg, *supra* note 15, at 98 ("imperfect 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").

[139] *See*, *e.g.*, Emily Steel et al., *How much is your personal data worth?*, FIN. TIMES (June 12, 2013), ig.ft.com/how-much-is-your-personal-data-worth/; Ignacio N. Cofone, *Why Paying for Facebook Won't Fix Your Privacy*, VENTUREBEAT (Apr. 17, 2018), venturebeat.com/2018/04/17/why-paying-facebook-wont-fix-your-privacy/.

[140] Strandburg, *supra* note 15 at 134–141 (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").

[141] Strandburg, *supra* note 15, 130–152 ("[I]t is nearly impossible for a consumer to estimate the increment of expected harm associated with a given instance of data collection."); Cofone & Robertson, *supra* note 83.

[142] This aggregation problem relates to the dignity-based criticism of data as property. *See* Bietti, *supra* note 96, at 13* ("subjecting and devolving large amounts of personal data to market forces could be said go against our dignity … the combination of data that comes to form a profile about us may be of the inalienable kind and its arbitrary disposal impermissible").

[143] *See generally* Bietti, *supra* note 96, at 7* ("a lot of data is created unintentionally, by corporate and non-corporate entities and individuals, as part of a diffuse system that captures it without a specific purpose for doing so.").

[144] *Id.* at 19.

to consider that personal data is a public good.[145] Consent of any person becomes irrelevant as one aggregates people to the dataset and infers, probabilistically, personal information about each person based on the information disclosed by others.[146] In other words, information is not a distinct commodity because it can be held by several agents at the same time, 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. These characteristics make personal information unfit for *in rem* rights and for individual-consent-based property rules.

A consequence of the informativeness of our information 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.[147] No data is only about one person. 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[148]— the power to exclude cannot be given to everyone involved in the information.

An extension of this problem is the under-protection of anonymized data.[149] Privacy statutes do not protect data without identifiers. But so-called anonymous datasets hold enormous power, and there are group harms that come from them. 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,

---

[145] Schwartz, *supra* note 42, at 2084; Ignacio N. Cofone, *The Dynamic Effect of Information Privacy Law*, 18 MINN. J.L. SCI. & TECH. 517, 530–31 (2017).

[146] Barocas & Nissenbaum, *supra* note 72 (explaining consent becomes meaningless as someone aggregates people to the data); Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039 (2017) (explaining how information about someone is inferred probabilistically based on information provided by them and others); Purtova, *supra* note 128 (explaining this in terms of network effects).

[147] Spiekermann et al., *supra* note 120, at 7.

[148] 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).

[149] 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).

allowing inferences for members of such groups.[150] 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. Every decision about data has—and it would continue to have under a property rule—spillover effects towards others. This has led some commentators to characterize personal information as a public good or 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.[151]

Moreover, data can always be re-identified.[152] 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 and then can be de-anonymized, becoming harmful—both in the privacy harm that re-anonymization involves per se and the external harms that can accrue from it.

From a process point of view, the idea of data as labor diverges here because it seemingly validates control over aggregated data (inferred data) by data aggregators by arguing that, because they invested labor into creating it, they are more deserving of having control.[153] That is, the lack of protection for aggregated 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 data 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.[154]

---

[150] GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (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).

[151] Schwartz, *supra* note 42, at 2084; Nadezhda Purtova, *Property Rights in Personal Data: Learning from American Discourse,* 25 COMP. L. & SEC. REV. 507, 519 (2009); Spiekermann et al., *supra* note 120, at 5.

[152] Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security Myths and Fallacies of "Personally Identifiable Information"*, 53 COMM. ACM 24 (2010), www.cs.cornell.edu/~shmat/shmat_cacm10.pdf.

[153] ERIC POSNER & E. GLEN WEYL, RADICAL MARKETS 205–249 (2018).

[154] Bietti, *supra* note 96, at 19*.

Data, in other words, is much about inferences.[155] Even if it were true that data subjects made rational and informed 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.[156]

Two recent cases illustrate this dynamic. In *Meyers v. Nicolet Restaurant*, a restaurant allegedly violated FACTA by printing the expiration date of a credit card on a sales receipt.[157] 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. [158] 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 printed, the information is also stored in the system. 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 problem of data aggregation, it may be easy for them to duplicate credit cards. If that happens, it will be extremely difficult for consumers to trace back the duplicated credit cards to the aggregation of different pieces of extra credit card information from the different restaurants.[159]

---

[155] Cofone & Robertson, *supra* note 83 at 1475.

[156] Barocas & Nissenbaum, *supra* note 72, at 32 (discussing what we learned from Target's "infamous pregnancy prediction score" incident).

[157] Meyers v. Nicolet, 843 F.3d at 725 ("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").

[158] Kirchein v. Pet Supermarket, Inc., 297 F. Supp. 3d at 1356 ("Kirchein filed a putative class action alleging that the Defendant violated the Fair and Accurate Credit Transactions Act, 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'").

[159] Danielle Citron & Daniel Solove, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 756–57 (2018)("A problem is that fraud may not surface until after an identity thief combines leaked personal data with other information").

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

* * *

Consent-for-use is the system that we already have for privacy, and privacy scholars have shown that it does not work. Data property, by placing further weight on consent-for-use, would not improve the status quo. A property-rule regime would establish that companies would not be able to use individuals' data unless those individuals consented to the use. But consumers already do this. They consent to websites' and apps' terms of service. The ineffectiveness of data property is not theoretical, but one that is actualized.

V. WHY THE PROPERTY CONCEPTION IS SELF-DEFEATING

In addition to exacerbating these pre-existing problems so far raised in other privacy law contexts,[160] data property contains a fatal flaw: it produces a moral hazard problem. In contrast to existing property criticisms, which show how the property conception of data is trying to achieve the wrong goal,[161] and newly applicable criticisms, which show that the property conception is ineffective at protecting people's privacy,[162] the moral hazard problem means that the property conception is counterproductive at doing the very thing it tries to do: increasing user control.

---

[160] *See supra* Part IV.
[161] *See supra* Part III.C.
[162] *See supra* Part IV.

A. Moral hazard in privacy law

i. The Grindr hazard

In January 2021, queer dating app Grindr faced a historic fine of 10% of its global turnover by the Norwegian Data Protection Authority.[163] 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 their privacy policy, the Authority ruled, was insufficient due to Grindr's information's sensitivity, which includes sexual orientation and HIV status.[164] 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 the users to their website.[165] The plaintiffs alleged that the collection and unauthorized disclosure led to feelings of being under surveillance. Why was Grindr and Google users' well-being affected, a reader may ask, 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.[166]

---

[163] Finn Myrstad & Øyvind H. Kaldestad, *Historic Victory for Privacy as Dating App Receives Gigantic Fine*, FORBRUKERRADET (Jan. 26, 2021), www.forbrukerradet.no/news-in-english/historic-victory-for-privacy-as-dating-app-receives-gigantic-fine/ (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"); .

[164] *Norwegian DPA: Intention to issue € 10 million fine to Grindr LLC,* EUROPEAN DATA PROTECTION BOARD, (Jan. 26, 2021), edpb.europa.eu/news/national-news/2021/norwegian-dpa-intention-issue-eu-10-million-fine-grindr-llc_en.

[165] Frank v. Gaos, 139 S. Ct. 1041, 1044 (2019).

[166] *See* Paul Milgrom & John Roberts, *Moral Hazard and Performance Incentives*, *in* ECONOMICS, ORGANIZATION AND MANAGEMENT 166–170, 179, 185–190 (1992) (explaining how moral hazard leads to perverse risk incentives); John Marshall, *Moral Hazard*, 66 AM. ECON. REV. 880 (1976) (introducing the seminal contribution for moral hazard in economics); David Rowell & Luke Connelly, *A History of the Term "Moral Hazard"*, 79 J. RISK & INSUR. 1051, 1051–58, 1064–69 (2012) (explaining the historical evolution of the term and the differences between its colloquial and economics uses).

A common type of moral hazard are principal-agent problems, 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).[167] 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).[168]

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 does (in this case the company).[169] If both parties could know in advance and be able to observe later on the agent's risk-taking behavior, they could try to add a contractual clause that internalizes the risk.[170] But one of those parties (in this case, the consumer) is unable to do so because of the information asymmetry.[171]

Because one of those parties (the consumer) does not know when the other one (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.[172] This is a problem in areas where the first

---

[167] John Armour et al., *Agency Problems and Legal Strategies*, *in* THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH 29–45 (Reinier Kraakman et al. eds., 2017) (explaining how principal-agent problems are a type of moral hazard problems).

[168] *Id.* (explaining how moral hazard's incentive problems exist in principal-agent problems).

[169] Bengt Holmstrom, *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).

[170] Sugato Bhattacharyya & Francine Lafontaine, *Double-sided moral hazard and the nature of share contracts*, 26 RAND J. ECON. 761, 766–775 (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. BEHAVIOR 544, 550–57 (2018) (showing in an experimental setting that contractual bargaining is desirable, when possible, to solve hidden action moral hazard).

[171] Holmstrom, *supra* note 166.

[172] 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 wellbeing is affected by the second party's behavior after the interaction.

ii. Perverse corporate incentives

This lack of incentives to take care ex-post has been considered a drawback of property rules in other areas of the law where parties are affected by the interaction after it happens. For example, it has in environmental law, particularly for the calculations of carbon dioxide emissions.[173] When there is a lack of ex-post restrictions and monitoring, there are 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.[174]

This moral hazard problem would affect 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, continues to affect the data subject's interests and wellbeing, as the Grindr example illustrates. This is because personal information inevitably retains a connection to the person even after they no longer control it.[175]

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 (shirk). This is because the cost of such safeguards is borne by corporations, while the benefits are borne by data subjects, so

---

[173] *See* Jean-Jacques Laffont, *Regulation, Moral Hazard and Insurance of Environmental Risks*, 58 J. PUB. ECON. 319, 322–24 (1995); Anastasios Xepapadeas, *Environmental Policy under Imperfect Information: Incentives and Moral Hazard*, 20 J. ENVTL. ECON. MGMT. 113, 113–115 (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).

[174] *Id.*

[175] Mark Verstraete, *Inseparable Uses*, 99 N.C. L. REV. 427, 466–67 (2021) ("Use restriction are necessary for governing personal data because, unlike paradigmatic commodities, personal data retains a connection to specific people that survives transfer" at 467).

there is no economic reason for corporations to have these safeguards other than compliance with regulations or a tenuous benefit over competitors from a reputation standpoint.[176]

Second, they have incentives to over-process information and give it away for profit independently of the risk that this may create for consumers, consequently driving up harm (expropriate). 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 person, 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

An ameliorated version of this market failure already exists under current privacy law to the extent that it relies on consent at the moment of collection as a protection mechanism. It would be aggravated if we relied on data property for data subjects' protection. If data collectors must only compensate data subjects in some way to obtain consent to collect their personal information (for example by providing them a service), then data collecting companies have no incentives to incur costs of care or to moderate activity levels (information processing) to avoid them risk. This problem arises because property rules are satisfied only at the start, allowing the acquirer to forget about potential externalities later on—unlike liability rules, which can impose costs at all moments of the decision-making process.[177]

---

[176] *See* Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, U. ILL. L. REV. 1, 42* (forthcoming 2021) (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.

[177] Calabresi & Melamed, *supra* note 8.

This market failure would defeat any permutation of data property even if data subjects had perfect information, were fully rational, and could therefore engage in capable privacy self-management. This is so because it 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.

Moreover, even if, having full information, data subjects could calculate the expected externalities into their compensation for data, this would not solve the problem, as 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, consequently, they would increase the price demanded for their personal information in accordance with those increased risks.[178] The price increase would reduce the demand for such information in equilibrium, which would reduce the supply of information to meet that demand.[179] 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 data subjects do not act in a fully informed and rational way, so they do not adjust for expected risk.[180] 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 precisely 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, among others, re-identified if the collected data was at some point de-anonymized. These are measures that may increase expected harm for data subjects more than they increase expected benefits for companies processing data, but

---

[178] STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 206–227 (1987) (describing insurance and the allocation of risk).

[179] *See* Murphy, *supra* note 42, at 2385 (describing the "efficiency loss" associated with inhibited information disclosure due to higher cost).

[180] Ignacio N. Cofone, *The Value of Privacy: Keeping the Money where the Mouth is*, 2015 PROC. WORKSHOP ON ECON. INFO. SECURITY 1 (2015).

companies have incentives to engage in the socially inefficient behavior because they can externalize this cost.

C. Transaction costs in privacy under moral hazard

From an economic standpoint, one could wonder: if property rules are traditionally 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?

Here one must recall that the cost of people's personal information for them is the expected cost of harmful processing, such as discrimination, or harmful disclosure, such as a breach. The more personal information is processed, the higher the expected cost of it. Even absent the moral hazard market failure, for a property rule to work, data subjects would have to know the expected cost of their information in advance to ask for an equivalent price and be compensated.[181]

Privacy harm often involves several potential parties who are unidentifiable ahead of time, many of whom only come into contact with the data ex-post.[182] 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 rule to protect 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 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 positioned to do something about it and improve their situation.

---

[181] Cofone, *supra* note 96 at 524–27 (discussing "concealment and asymmetric information").

[182] Amy Kapczynski, *The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism*, 59 UCLA L. REV. 970, 1009 (2011) (explaining that the cost of protecting private information "requires more than relying on formal individual consent").

In sum, unlike other things that are typically property, data have the capacity to affect the data subject's interest after transfer. Data property can protect from 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.

VI. EXPANDING PRIVATE RIGHTS OF ACTION

Liability rules allow for ex-post compensation based on harm; and the risk of that harm is completely dependent on the corporation, not the data subject. Liability addresses the moral hazard problem because it causes corporations to internalize the risk. It also compensates data subjects for the resulting harm and not just for the value they set on data at the time it is collected – data subjects are likely to undervalue their data anyway because of being unaware of the magnitude of potential risk. But private rights of actions are not a given in statutory privacy. They are contemplated in the Virginia's CDPA,[183] but only for security breaches in the CCPA and the California Privacy Rights Act. They are contemplated in some, but not all, of state proposed bills. [184]

---

[183] Consumer Data Protection Act, H.B. 2307, 2021 Sp. Sess. §§ 59.1–574(1), (2) (Va. 2021), lis.virginia.gov/cgi-bin/legp604.exe?ses=212&typ=bil&val=hb2307.

[184] They are contemplated in the New York Privacy Act, and the Oklahoma Computer Data Privacy Act; they are not included in the Alabama Consumer Privacy Act, Utah's Consumer Privacy Act, or the Washington Privacy Act. *See* New York Privacy Act, A. 680, 2021-2022 Leg., Reg. Sess. § 1104(b), www.nysenate.gov/legislation/bills/2021/A680 (establishing that controllers must notify consumers of "the purposes for which the categories of personal data is used and disclosed to third parties"); § 1103.3(a)(i) (requiring that controllers delete the consumer's personal data on request where the data "is no longer necessary in relation to the purpose for which the personal data was collected or otherwise processed"); Oklahoma Computer Data Privacy Act, H.B. 1602 (2021); Alabama Consumer Privacy Act, H.B. 216 (2021); Consumer Privacy Act, S.B. 200 (2021); Washington Privacy Act, S. 5062, 67th Leg., Reg. Sess. § 101(6), § 107(2), § 107(4), http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062-S.pdf?q=20210125113540

A. The benefits of privacy liability

i. Addressing property's problem

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

Instead of choosing whether to allow any type of processing and suffer the costs of the consequences later on, under liability rules data subjects would be compensated if any collection or processing resulted in harm, for example by causing financial damage (e.g., by identity theft),[185] reputational damage (e.g., through the dissemination of embarrassing information),[186] physical harm,[187] or discrimination.[188]

Liability rules would in such a way avoid the problems of property rules identified above. Liability rules are transactional rules that are useful when transaction costs are high.[189] The information asymmetry between data subjects and companies operates as transaction costs: as a

---

[185] *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), www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[186] *See* Cofone & Robertson, *supra* note 97 (arguing that privacy harm and reputational harm are conceptually distinct but are both protected by privacy rules).

[187] Mary Anne Franks, *Sexual Harassment 2.0 Special Feature: Cyberlaw*, 71 MD. L. REV. 655, 657–658 (2011); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 5–8 (2016).

[188] *See* Ignacio N. Cofone, *Antidiscriminatory Privacy*, 72 S.M.U. L. REV. 139 (2019) (arguing that privacy rules can be used to prevent discrimination). *See also* Fair Housing Council of San Fernando Valley v. Roommates.com LLC, 521 F.3d. 1157 (9th Cir. 2008).

[189] *See* Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027, 1036–1072 (1995).

consequence, data subjects face information acquisition costs that make it difficult for them to reach welfare-enhancing transactions.[190]

Property rules' ineffectiveness due to asymmetric bargaining positions would therefore be remedied by liability rules' "collectively defined prices," namely, ex-post compensation. Defining compensation ex-post based on harm, as opposed to doing it ex-ante based on bargaining, maintains compensation for the risks that data subjects are exposed to while avoiding costly bargaining, which would be ineffective due to asymmetric information. Indeed, the standard rationale for suggesting the use of liability rules over property rules as a transactional rule is the costliness of ex-ante bargaining.[191]

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. For this reason, negotiating over one's information has high transaction costs—even when the costs of surveillance and communication are low.[192] In other words, even if the information and power asymmetries did not exist, people would have high costs to bargain over their data because they would have to do so with countless parties. The relevant costs to determine which transfer rule should protect 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.

Fixing damages in accordance with the harm caused would also solve the property rule's under-protection of information obtained through data aggregation and re-identification.[193] Aggregation, as seen above, presents a problem for effective form of protection through property rules because the cost for the data subject of each piece of information is irrelevant. What is relevant is the cost they face for aggregated information including the inferences made possible by such aggregation, for which under property rules they would obtain no compensation. Liability rules do not face this problem because they can set ex-post

---

[190] Litman, *supra* note 102.
[191] Calabresi & Melamed, *supra* note 8, at 1110.
[192] *See* Kapczynski, *supra* note 178, at 1009 (explaining that the cost of protecting private information "requires more than relying on formal individual consent").
[193] *See* Calabresi & Melamed, *supra* note 8, at 236 n.3 (stating that, under liability rules, "even if damages are set imprecisely, liability rules can induce beneficial nonconsensual taking").

compensation in expectation equal to the harm. Conversely, the expected cost of a liability rule 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, then the externalities present in the moral hazard problem 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 over-process data and to invest in reasonable security measures because harming data subjects would be expensive.[194]

Liability rules correct the moral hazard problem in an orthodox way: deterrence. This mechanism is analogous to fiduciary law and corporate law. There, the fiduciary's duty of care deters ex-post risky behavior in order to correct a moral hazard problem between the principal and agent in the first and between the shareholders and the board of directors in the second.[195]

Data property is not only ineffective at achieving control. It is an ineffective protection mechanism because it is too loosely tied to harm prevention. If consent is established as a mechanism to help consumers manage their data risks to prevent harm from taking place, it has failed miserably. And if the opposite is true, and consent is a mechanism to allow companies to harm consumers by complying with checkboxes, what is the point?

---

[194] 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 moral hazard problems.

[195] Robert H. Sitkoff, *The Economic Structure of Fiduciary Law*, 91 B.U. L. REV. 1039, 1042–45 (2011) (explaining fiduciary obligations, liability, and deterrence in fiduciary law); Frank H. Easterbook & Daniel R. Fischel, *Corporate Control Transactions*, 91 YALE L.J. 698, 702 (1982) (explaining fiduciary obligations, liability, and deterrence in corporate law).

ii. Accounting for consumers' risk preferences

Besides addressing property rules' gaps, liability rules would present an advantage regarding risk aversion. If data subjects are more risk-averse than corporations, liability rules may be in the interest of both players in the interaction even besides their ability to solve the moral hazard problem.[196]

If the amount of compensation is determined by the ex-ante expected harm as it would be under property rules, risk aversion becomes important. 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, based on the problems above, it may not) that value would be higher for the "seller" (data subject) than for the "buyer" (data collector) due to the risk averseness of the former. Full ex-post compensation, that is, paying for the amount of harm once it happens as opposed to for the expected harm in advance (whether it happens or not), would therefore be more valuable for data subjects than ex-ante compensation.[197]

If the compensation did take this into account and was higher than the expected harm to account for the disutility of risk (taking from some surplus and leaving data subjects indifferent between ex-ante and ex-post compensation) then a liability rule would also be cheaper for data collectors than a property rule. Even under the most expensive type of liability for companies, strict liability, the rule's expected cost would not by definition exceed the expected cost of harm.

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. As, under a property rule, compensation should be added for the disutility of risk, any type of liability including strict liability is cheaper for companies than a properly executed property rule. Any industry argument in favor of property rules over strict liability necessarily relies on externalities imposed on data subjects.

---

[196] *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).

[197] SHAVELL, *supra* note 174 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.").

After determining through what mechanism the right is transferred and how to define compensation for it under liability rules, the next question concerns which type of liability is the most appropriate for privacy: negligence, strict liability, or anything in between (such as comparative negligence or strict liability with a negligence defense).

iii. Objections to liability

An objection to these liability rules is that privacy harm is often difficult to detect and remedy. Big data reduced the costs of surveilling people and it allowed for aggregating personal data to create new data, thereby introducing a host of new types of privacy harm.[198] When a website makes a ghost profile with someone's name on it but they lack evidence of reputational damage, such as it happened in *Spokeo v. Robins*, courts are unsure of whether to grant them remedy.[199] When a credit bureau is hacked but victims lack evidence that this has caused them financial damage, such as in the Equifax hack, courts are unsure of whether to grant them remedy.[200]

While an in-depth exploration of this objection is better suited for a different article,[201] one thing is certain: privacy harm is easier for courts and enforcement authorities to identify after-the-fact than it is for consumers to anticipate before-the-fact. There are frameworks for assessing privacy harm after the fact that courts and regulators can use.[202] But no one can anticipate it effectively, much less consumers with insufficient information and no bargaining power. And the burden of anticipation adds the wrong incentives to take care after the fact when no such after the fact assessment is given.

A second objection is that relying on liability rules that depend on harm may run on problems of federal jurisdiction in terms of Article III

---

[198] Citron & Solove, *supra* note 156, at750–57 .
[199] *See*, *e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).
[200] Editorial, *The Unfinished Business of the Equifax Hack*, BLOOMBERG (Jan. 29, 2019), www.bloomberg.com/opinion/articles/2019-01-29/equifax-hack-remains-unfinished-business.
[201] *See* Ignacio N. Cofone, *Privacy Class Actions* (draft 2021, on file with author).
[202] Cofone & Robertson, *supra* note 102 at 1049–58 (presenting a model of privacy harm); Citron & Solove, *supra* note 156 at 27–34 (presenting a approach for assessing risk and anxiety harms).

standing according to the landmark privacy standing case *Clapper v. Amnesty International*.[203] In an ideal world, the moral hazard problem should lead federal courts would revise and expand their standing doctrine for privacy harms. But in the meantime, state courts hold an enormous power to do this. Some of the most consequential privacy cases have come from state courts. For instance, in *Rosenbach v. Six Flags*, the Illinois Supreme Court rules 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.[204] And the role of state courts in privacy will continue to grow as statutes tabled this legislative year across the country continue to pass.

B. How to implement privacy liability

i. Liability rules as private rights of action

So far, this Part has shown why, to adequately protect privacy rights, one should incorporate a combination of property and liability transfer rules for rights over people's personal information. The smallest incremental change that would achieve this is keeping consent-based safeguards while enhancing the scope of private rights of action and compensable harm.

Incorporating liability rules for personal information could be achieved by creating a separate, harm-dependent private right of action in privacy statutes such as the CCPA and CDPA. This liability system is already in place for data breach notifications,[205] and it could be expanded.

---

[203] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401-09 (2013). *See also* Bradford Mank, *Clapper v. Amnesty International: Two or three Competing Philosophies of standing Law?"*, 81 TENN. L. REV. 211, 213, 255 (explaining that the Supreme Court held in Clapper that Article III's language imposes standing requirements for plaintiffs before federal courts can consider the merits of a case; demonstrating that there has been considerable debate about the extent to which Congress may enlarge the definition of concrete injury under Article III by statute, and the extent to which the separation of powers limits Congressional authority to grant universal standing rights to plaintiff 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).

[204] Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Ill. Sup. Ct. 2019).

[205] Citron & Solove, *supra* note 156 at 739–41 ("In the past two decades, plaintiffs in hundreds of cases have sought redress for data breaches caused by inadequate

But it could also be achieved absent a legislative process by expanding the privacy tort to complement regulatory measures.[206] That is, 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.[207] Second, by interpreting that privacy statutes such as the CCPA and CDPA do not pre-empt this amplified privacy tort.

This system would not be unique to privacy. This is common practice when administrative and tort law are combined to prevent and compensate harm. 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.[208] State traffic law authorities, similarly, sanction individuals for driving with a broken light even when they did not get into an accident because of it.[209] But none of these administrative regulations pre-empt compensation when harm occurs.

Courts interpreting privacy law could similarly enforce sanctions for processing people's personal information without justification as stipulated by statute while giving individuals a common law remedy to

---

data security" at 740); William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (describing the process by which "reasonable security practices" developed).

[206] *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1828–1852 (2010) (proposing a number of ways to expand the privacy tort and complement it with other torts to cover new ground); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 145–156 (2007) (explaining the evolution of common law privacy). *But see* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. 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 harms to privacy and reputation in the digital age).

[207] *See* Jane Y. Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 209–210, 238 (2012) (arguing that intrusion upon seclusion targets privacy concerns in the information stage and that enforcement of seclusion can expand significantly).

[208] Toxic Substances Control Act § 2641, 15 U.S.C. § 2514 (2018) www.govinfo.gov/content/pkg/USCODE-2018-title15/pdf/USCODE-2018-title15-chap53.pdf; Federal Water Pollution Control Act § 309, 33 U.S.C. § 1251 www.waterboards.ca.gov/laws_regulations/docs/fedwaterpollutioncontrolact.pdf/.

[209] *See*, *e.g.*, Motor Vehicles and Traffic Act, GA. CODE ANN. § 40-8-20 (2010); N.Y. Vehicle and Traffic Law, § 375(2)(a), http://ypdcrime.com/vt/article9.htm#t375-2a1; WASH. REV. CODE § 46.37.040 (1977), app.leg.wa.gov/RCW/default.aspx?cite=46.37.040.

obtain compensation when harmed. In the European Union and adequacy countries, privacy law would then 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.[210] In both cases, this would complement statutes that are focused on prohibited behavior with private law lawsuits focused on harmed individuals.[211]

ii. Determining the appropriate standard

In privacy, the potential tortfeasors (data collectors and data processors) are the only parties to the interaction that can exert any significant control over the probability of harm occurring and, in the extent that it does, the amount of harm.[212] This is unlike most types of accidents considered by tort law.

Liability rules aim to place the burden of care on the party who can control the probability of the accident taking place.[213] An accident taking place depends on two things: levels of care and levels of activity.

The advantage of negligence rules is that they induce an appropriate level of care from the victim and tortfeasor (but not activity), while the advantage of strict liability is that it induces an appropriate level of both care and activity by the tortfeasor (but not the victim).[214] The tort

---

[210] Michael Greeve, *The Private Enforcement of Environmental Law*, 65 TUL. L. REV. 339 (1991) (explaining how Congress partially relies in private enforcement for public environmental law objectives); Kai Huschelrath & 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).

[211] In terms of legislative reform, statutes can help overcome the difficulties that courts face in this space by making an explicit choice on non-pre-emption, choosing between negligence and strict liability, and providing clarity in how privacy harm should be estimated.

[212] *See* Chris Jay Hoofnagle, *Internalizing Identity Theft*, 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").

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

[214] STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 5–46 (1987) (introducing the theory of liability and deterrence in accident law).

law 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.[215] Therefore, the question about which rule is most appropriate is the 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).[216]

Strict liability sets adequate 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 fully internalized.[217] If harm occurs, under strict liability the tortfeasor has an obligation to remedy no matter what happens.[218] Thus, tortfeasors are more likely to take eventual harms into account under strict liability than they are under a liability regime in which only on some occasions they will be responsible for such harm. Negligence, on the other hand, can induce an adequate level of care by both parties but not an adequate level of activity. Compared to strict liability, negligence leads to appropriate care by the victim but, in unilateral accidents, the victim's care is irrelevant.

In technical terms, privacy harm is produced in unilateral accidents.[219] After data are disclosed, they leave the data subjects' sphere of control, thereby also rendering them unable to control the probability of harm.[220] The protection mechanisms that data subjects can use after data are disclosed have a negligible influence on the probability of data breaches compared to the security measures that data processors can implement.[221]

In addition, both the level of care and the activity levels of corporations are relevant for the probability of data harm materializing.[222] The types of processing and level of database security (care level), as well

---

[215] *Id.* at 73–104 (exploring factors bearing on the determination of negligence).
[216] *Id.* at 73–104.
[217] Steven Shavell, *Strict Liability versus Negligence*, 9 J. LEGAL STUD. 1 (1980).
[218] Richard A. Epstein, *A Theory of Strict Liability*, 2 J. LEGAL STUD. 151 (1973).
[219] Cofone & Robertson, *supra* note 97, at 1049–53 (modelling privacy loss).
[220] *See* Hoofnagle, supra note 263, at 1 ("One faction explains the identity theft as a problem of a lack of control over personal information").
[221] Hoofnagle, *supra* note 263, at 34–36 (discussing internalizing externalities in the context of security measures intended to prevent identity theft.
[222] *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").

as the amount of processing and number of data transfers (activity levels), directly affect the probability of data subject harm.[223]

This is important for the choice of liability rule. The application of a negligence standard to liability for data breach notifications,[224] and for data security generally,[225] 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 uncertainty.[226] From this 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.[227]

For these reasons, a strict liability rule would, at least in principle, internalize the externalities of moral hazard and induce appropriate levels of care and activity.

---

[223] *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.").

[224] Mark Verstraete & Tal Zarsky, *supra* note 173, at 32–35*; Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data, Breaches,* Yale L.J. Forum, 614 (Jan. 11, 2018).

[225] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CALIF. L. REV. 241, 261–8 (2006);

[226] 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 263, at 32–35 (suggesting strict liability for identity theft).

[227] *See* Ian Ayres & Eric Talley, *Distinguishing between Consensual and Nonconsensual Advantages of Liability Rules*, 105 YALE L.J. 235 (1995); Louis Kaplow & Steven Shavell, *Do Liability Rules Facilitate Bargaining? A Reply to Ayres and Talley*, 105 YALE L.J. 221 (1995); Ian Ayres & Jack Balkin, *Legal Entitlements as Auctions: Property Rules, Liability Rules, and Beyond*, 106 Yale L.J. 703, 717-733 (1997) (describing the nonconsensual advantage of second-order liability rules); Ian Ayres & Paul 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).

C. Combining public enforcement with private claims

i. A mixed enforcement system

Most privacy statutes evaluate harm through regulated conduct: it does not matter whether a victim was harmed, but whether someone behaved in a way forbidden by the regulation (ex-ante).[228] While this paradigm has its benefits,[229] including the capability for large-scale deterrence, it is difficult to achieve compensation together with deterrence when only fines are prioritized as an enforcement mechanism. Public regulatory enforcement by itself cannot sufficiently provide victims with compensation.

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."[230] Privacy torts are not new.[231] In the past, privacy problems were indeed addressed through tort law. People sued when someone opened their letters, broke into their home, or went through their financial papers, as well as when someone disclosed harmful secrets to others.[232]

---

[228] *See* Janet Walker, *Facebook v. Douez and Privacy Class Actions, in* CLASS ACTIONS IN PRIVACY LAW 68–69 (Ignacio N. Cofone ed., 2020) (discussing statutory privacy in Canada).

[229] This approach has a key benefit: it avoids the difficult question of privacy harm. But it also has a cost: it will sanction individuals and companies when they do not produce harm, and it will fail at sanctioning them in situations in which they do. An example of the first is Lindqvist. An example of the second are the countless meaningless manifestations of consumer consent to process data in ways that are harmful to them, particularly in jurisdictions that focus on consent but not on its meaningfulness.

[230] Ari Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 2, 40 (2020).

[231] See Citron & Solove, *supra* note 156, at 782 ("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").

[232] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century*, 98 CALIF. L. REV. 1887 (2010).

For these reasons, both public and private enforcement are needed in practice to overcome the information and power asymmetries that exist for citizens and consumers in data collection, processing, and use. Together with public enforcement, in other words, private rights of action are a key legal tool for citizen and consumer data protection.[233]

ii. Statutory precedent

Some state privacy statutes give rise to direct private rights of action. Some examples are Washington D.C.'s *Use of Consumer Identification Information Act*,[234] and Illinois' *Biometric Information Privacy Act*,[235] which famously triggered the lawsuit against Six Flags,[236] and more recently, triggered a class action lawsuit against Clearview AI for building one of the largest facial recognition databases in history.[237] The CCPA creates civil penalties and a form of private right of action for violations of the statute that give consumers some ability to bring civil suit for actual or statutory damages, whichever is greater, for claims related to data security breaches,[238] but it lacks private rights of action to enforce most of its elements.[239]

Abroad, privacy claims in privacy law are currently based on a legal framework that makes it difficult for individuals to bring deserving claims successfully. For example, in Canada, starting a claim under PIPEDA is a long process: one must first report it to the OPC, wait for the office to investigate and release a report, and then start a *de novo* application in court.[240]

While cases based on these regulations are not frequent, some provisions provide space for them, and some cases do exist. The GDPR

---

[233] *See* Walker, *supra* note 286, at 68–69.
[234] *See*, *e.g.*, Hancock v. Urban Outfitters, Inc., 830 F.3d. 511 (D.C. Cir. 2016).
[235] Biometric Information Privacy Act, Pub. L. No. 95-994, 740 ILCS 14/1.
[236] Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Ill. Sup. Ct. 2019).
[237] David Mutnick v. Clearview AI, Inc., N.D. Ill. Case No. 20 C 0512 (2020) (refusing to dismiss the class action).
[238] CALIF. CIV. CODE §§ 1798.150, 1798.155(a), (b).
[239] Anupam Chandler, Margot Kaminski & William McGeveran, *Catalyzing Privacy Law*, MINN. L. REV. 1*, 21* (forthcoming 2021).
[240] Office of the Privacy Commissioner of Canada, *Enforcement of PIPEDA* (Apr. 4, 2020), at www.priv.gc.ca/biens-assets/compliance-framework/en/index

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.[241] However, as of today, there is little precedent on this front, and almost all of it stems from behavior that breached the GDPR under art. 82(1) and produced material harm, with immaterial having virtually no traction in courts, and both material and immaterial harm without a statutory breach not being contemplated.[242] This is key because the courts of Member States are the ones that determine the scope and meaning of "material and non-material damages" and how much compensation is appropriate for them.[243]

This traction has mainly taken place in The Netherlands,[244] Germany,[245] and Austria.[246] The United Kingdom, similarly, has seen

---

[241] Gabriela Zanfir-Fortuna, *Article 82*, *in* THE EU GENERAL DATA PROTECTION REGULATION: A COMMENTARY (Christopher Kuner, Lee A Bygrave and Christopher Docksey eds., 2020). *See also* GDPR art. 82(1).

[242] Eoin O'Dell, *Compensation for non-material damage pursuant to Article 82 GDPR*, CEARTA.IE (2020), http://www.cearta.ie/2020/03/compensation-for-non-material-damage-pursuant-to-article-82-gdpr/.

[243] Eoin O'Dell, *Compensation for Breach of the General Data Protection Regulation*, 40 DUBLIN U. L.J. 97, 115 (2017) (adding that the fact that this is a state-by-state approach means that private enforcement will be uneven unless cases reach the CJEU).

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

[245] *See* Jan Spittka, *Germany: First Court Decision on Claims for Immaterial Damages under GDPR*, DLA PIPER: PRIVACY MATTERS (Dec. 12, 2018), <blogs.dlapiper.com/privacymatters/germany-first-court-decision-on-claims-for-immaterial-damages-under-gdpr/>. 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), openjur.de/u/2116788.html; Karlsruhe Regional Crt. (Landgericht), 2019 8 O 26/19 (DE), dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Karlsruhe&Datum=02.08.2019&Aktenzeichen=8%20O%2026%2F19.

[246] Innsbruck Higher Regional Crt. (Oberlandesgericht), 2020 1 R 182/19b (AT), at www.dataprotect.at/2020/03/06/post-schadenersatz/. Note that the Higher

cases in small claims courts based on regulation 22 of the *Privacy and Electronic Communications Regulations 2003* (PECR) when a corporation acts in breach of the regulation, particularly when collecting information absent a lawful basis for processing.[247] Ultimately, Article 82(1) offers an ambiguous statement of claim for compensation that contributes to confusion when implemented by national courts.[248]

iii. Liability must depend on harm

These private rights of action are a type of liability-rule protection over privacy rights. In a property-rule 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 actions for breach of the regulation, versus private rights of action for the occurrence of harm. This mechanism can be read in terms of the normative considerations set above as a liability rule with a negligence standard, where compliance with the regulation is due care that exempts from liability.

For this idea to be 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 is to double down on consent and control and simply adding private enforcement. Doing so may be effective as a means of reducing the resources needed for data protection authorities, 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.

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.

[247] *See* Lloyd v. Google LLC, EWCA Civ. 1599 (2019) (holding that plaintiffs may recover damages for loss of control without proving pecuniary loss). Regulation 22 states that "(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender." *See also* Brendan Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 J. OF INTELL. PROP., INFO. TECH. & E-COM. L. 271 (2016).

[248] O'Dell, *supra* note 295, at 113–15, 147.

The only way to solve the moral hazard problem is to add liability rules to statutory privacy. And to add liability rules is to create liability for harm created independent of whether it was a consequence of regulatory breach. In other words, it is 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.

VII. BOLSTERING USE-RESTRICTIONS

As this Article showed, data property proposals aim to enhance something that privacy statutes and regulations have been doing all along: they rely on data subject control to protect their 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 is ineffective at avoiding harm.

The second way of increasing ex-post accountability is by bolstering use-restrictions in privacy law. The one, modest, use-restriction present in statutory privacy is the purpose limitation principle. Purpose limitation takes privacy law one step away from property rules. Purpose limitation is a way to reduce the moral hazard problem. The usefulness of the purpose limitation principle is illustrative of why property (transfer) rules as applied to data would not work. At the same time, the moral hazard problem is informative on how privacy statutes should delineate purpose limitation.

A. The usefulness of the purpose limitation principle

The principle is drawn from the Fair Information Practices Principles, which are the backbone of American privacy law.[249] It is one of the key provisions of the California Consumer Privacy Act (CCPA), the California Privacy Rights Act, and Nevada's Act to Protect the Privacy of

[249] Jones & Kaminski, *supra* note 18, at 99, 112 (2020).

Online Consumer Information. It is also so for the GDPR, and privacy legislation of countries that have or seek GDPR adequacy status.[250]

The purpose limitation principle is established by the CCPA when it refers to "compatible within the context in which the personal information was collected."[251] It is also included in Virginia's CDPA.[252] Far from being an obvious inclusion in states' privacy statutes, the principle is being debated in proposed bills across the country. State bills under consideration are divided as to including it. [253]

Abroad, purpose limitation is required by the GDPR by articles 5(1) and 6(4).[254] 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 purpose other than the one for which the personal data was originally collected under a set of requirements.[255] Further data processing is justified only on a new lawful basis for processing; that is,

---

[250] *See generally* ME KONING, THE PURPOSE AND LIMITATIONS OF PURPOSE LIMITATION (2020).

[251] CCPA, §1798.140(o)(2).

[252] Consumer Data Protection Act, H.B. 2307, 2021 Sp. Sess. §§ 59.1-574(1), (2) (Va. 2021), lis.virginia.gov/cgi-bin/legp604.exe?ses=212&typ=bil&val=hb2307 (containing similar statutory language to the Washington Privacy Act).

[253] The Alabama Consumer Privacy Act, the New York Privacy Act, Utah's Consumer Privacy Act, the Washington Privacy Act include it. But the Oklahoma Computer Data Privacy Act does not; neither do the statutes proposed in Kentucky and Minnesota. *See* Alabama Consumer Privacy Act, H.B. 216 (2021); New York Privacy Act, A. 680, 2021-2022 Leg., Reg. Sess. § 1104(b), www.nysenate.gov/legislation/bills/2021/A680 (establishing that controllers must notify consumers of "the purposes for which the categories of personal data is used and disclosed to third parties"); § 1103.3(a)(i) (requiring that controllers delete the consumer's personal data on request where the data "is no longer necessary in relation to the purpose for which the personal data was collected or otherwise processed"); Consumer Privacy Act, S.B. 200 (2021); Washington Privacy Act, S. 5062, 67th Leg., Reg. Sess. § 101(6), http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062-S.
pdf?q=20210125113540 ("Consent" must relate to a "narrowly defined particular purpose"); § 107(2) ("controller's collection of personal data must be limited to what is reasonably necessary in relation to the purposes for which the data is processed"); § 107(4) ("may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which the personal data is processed unless the controller obtains the consumer's consent"); Oklahoma Computer Data Privacy Act, H.B. 1602 (2021); H.B. 408 (2021) (Kentucky); H.F. 36 (2021) (Minnesota).

[254] Jones & Kaminski, *supra* note 18, at 112–15.

[255] *See* GDPR, art. 6(1)(a)–(e).

one of the legal grounds required to authorize the initial processing.[256] The prior 1995 Directive[257] also included a compatibility requirement,[258] but this requirement was removed later on when giving further precision to the 1995 Directive.[259]

These GDPR provisions are relevant to American law. The GDPR has also influenced the CCPA and CDPA, is likely to continue having a role in state and federal privacy statutes.[260] The GDPR is also directly relevant to American companies as, since the *Schrems II* case from this past July, they must comply with the GDPR when collecting, processing, or distributing personal information from European data subjects.[261]

Indeed, one of the key obstacles to obtaining facile consent that does not constitute meaningful consent is the importance of identified purposes.[262] Data protection agencies often find that data collection was unlawful because data subjects were unaware of the purpose for which their data were being collected. In 2011, for example, the Canadian Office of the Privacy Commissioner (OPC) found that a complainant was uninformed concerning the collection of her personal information because its purpose was unclear and vague.[263] In 2014, it asked an organization to

---

[256] 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. COMP. & TECH. 144 (2014).

[257] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, Council Directive 95/46, 1995 O.J. (L 281).

[258] *See Id.*, art. 6(1)(b).

[259] *See* GDPR art. 6(4) (giving the controller significant leeway to apply the subjective compatibility test to further process data).

[260] *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1711–13 (2020) (discussing the GDPR and CCPA in relation to principles for fair information processing).

[261] *See* Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd. [Maximillian Schrems], 2018 (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).

[262] *See* Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, EUROPEAN COMMISSION: JUSTICE AND CONSUMERS (Nov. 28, 2017), ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051; *Consent and Privacy*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May 2016), www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.

[263] *PIPEDA Report of Findings #2011-011: Public opinion research firm must better inform survey respondents about their personal information use; refrain*

translate its policy into French because the complainant was uninformed concerning the collection purpose of her personal information due to her limited understanding of English.[264]

The irony is that property rules in personal data are incompatible with a wide application of the purpose limitation principle. Property rules, including those over personal data, work based on the free transferability of the rights they protect,[265] making it more difficult to impose any restrictions ex-post.[266] Julie Cohen hinted at this idea when she argued 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."[267]

Notably, property rules allow for subsequent sales once information is acquired—as with any product where when one can re-sell an item after buying it.[268] In this way, property rules, while they may sound like the most consumer-protective, rather lower transaction costs for subsequent sales.[269] If companies have to ask data subjects for permission each time such information was traded, transaction costs are higher than with property rules.[270]

Property rules keep transaction costs relatively low precisely because consent needs to be acquired once, and not again for re-use or re-

---

from collecting full birth dates, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-011/ (last updated Apr. 9, 2013).

[264] *PIPEDA Report of Findings #2014-011: Investigation into the personal information handling practices of Ganz Inc.*, Office of the Privacy Commissioner of Canada (Oct. 7, 2014), www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-011/.

[265] Samuelson, *supra* note 75, at 1138–39 (using the language of property rights and identifying free alienation as a problem of property).

[266] Schwartz, *supra* note 42, at 2090.

[267] Cohen, *supra* note 10, at 1375.

[268] Peter 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).

[269] Cofone, *supra* note 96 at 543–44 (discussing the "non-collection default rule", a privacy rule).

[270] Swire, *supra* note 203 (stressing the importance of keeping overall prices low).

selling of the entitlement that was transferred through consent.[271] The purpose limitation principle removes this characteristic. The purpose limitation principle does so because it places a fundamental restriction on what can be done with the information later on: the company acquiring the information cannot simply use it or transfer it later on but needs a new agreement to do so.[272]

By removing the property-rule characteristic of acquiring consent only once, the purpose limitation principle reduces the moral hazard problem in two ways. The first is that it reduces the information asymmetry between consumers and companies. Moral hazard happens largely because of such information asymmetries.[273] By providing certainty about the uses that can be given to information, an important 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.[274]

The second is that it generates ex-post accountability. Such ex-post accountability reduces the moral hazard problem between companies and consumers because it places ongoing use restrictions on personal data. The principle does not eliminate the moral hazard problem, as companies can still use and transfer personal data in risky ways without internalizing such risk. But the scope of possibilities to do this becomes more limited. Reducing the scope of behavior from the more-informed party, as the purpose limitation principle does, is a way to reduce the moral hazard problem in economics literature.[275]

---

[271] Cofone, *supra* note 96, at 545 ("If companies had to ask Internet users for permission each time such information was traded, transaction costs would be too high, which would decrease information flow.").

[272] Liang Zeyu, *The Interpretation and Application of Purpose Limitation Principle in Personal Data Protection*, 5 J. COMP. L. (2018).

[273] Holmstrom, *supra* note 166, at 74 (showing that improving on imperfect information can reduce the moral hazard problem in principal-agent relationships).

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

[275] Patrick W. Schmitz, *Allocating Control in Agency Problems with Limited Liability and Sequential Hidden Actions*, 36 RAND J. ECON. 318 , 231–25 (2005) (discussing sequential agency problems' optimal organization).

B. Property and liability in purpose limitation

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[276]—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 transfer rules.

Intellectual property rights are transferred by a mix of property and liability rules.[277] Take the example of copyright. Regarding the property characteristics of copyright law, authors holding copyright are entitled to exclude others from copying their work.[278] 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,[279] partially alienating their exclusion right, and to request injunctions for the breach of such exclusion.[280] Regarding copyright's liability characteristics, authors face some compulsory licenses and have to accept fair use.[281] While compulsory licenses tend to be specific and limited, fair use is a central trait of copyright law.[282] In other words, purpose limitation allows for ongoing use-

---

[276] 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.

[277] *See* B.J. Ard, *More Property Rules than Property: Revisiting the Right to Exclude in IP*, 68 EMORY L.J. 685, 697–99 (2019) (describing the liability rule features of copyright).

[278] *See Id.*

[279] *See* WILLIAM CORNISH, DAVID LLEWELYN & TANYA APLIN, INTELLECTUAL PROPERTY: PATENTS, COPYRIGHT, TRADEMARKS AND ALLIED RIGHTS 525–30 (2013).

[280] *See* Ard, *supra* note 214, at 712–14 (arguing that copyright statutory damages awards are often high enough to function as property rules).

[281] Trotter Hardy, *Property (and Copyright) in Cyberspace: The Law of Cyberspace*, 1996 U. CHI. LEGAL F. 217, 233 (1996).

[282] *See* 17 U.S.C. § 107 (2012). *See also* Pierre Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1110–25 (1990) (discussing fair use's contours); Glynn 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).

restrictions, as opposed to permanent transfers—and these find 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 incurred in negotiating and monitoring the uses that it protects.[283] For example, the law allows quoting scientific works without the author's permission because obtaining such permission every time would create exceedingly high transaction costs, while citations do not harm the author's economic interest.[284] 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.[285]

Compulsory licenses, similarly, are a liability rule (them being compulsory means that the right-holder has no choice as to the transfer) designed to facilitate non-consensual use of an entitlement.[286] Compulsory license are usually set at actual damages (or an estimate of how the entitlement would be priced in a market transaction), which allows the user to engage in their use as long as it is efficient for them to pay that price.[287] These licenses under copyright law are somewhat analogous to the purpose limitation principle. Both of them specify the objective for which the information can be used and forbid its use for other purposes. An argument can be made for privacy law based on this similarity.

Because of its liability rule characteristic, the purpose limitation principle moderates the three problems set out in Part IV. The prohibition on asking consumers to agree to the use of data for any purpose is a limit on contractual freedom that at moderates the failings of notice and choice

---

[283] Wendy Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the "Betamax" Case and its Predecessors*, 82 COLUM. L. REV. 1600 (1982).

[284] In expectation, they do not reduce the expected number of copies sold—in fact, they may increase sales.

[285] 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 Raskind, *A Functional Interpretation of Fair Use: The Fourteenth Donald C. Brace Memorial Lecture*, 31 J. COPYRIGHT SOC'Y 601 (1983); Richard Posner, *When Is Parody Fair Use?*, 21 J. LEGAL STUD. 67 (1992).

[286] *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 (2012).

[287] *Id.*

and unequal bargaining position with regards to ongoing use of data. In the GDPR, purpose limitation prohibits bundling consent, which is a way to abuse the power and information asymmetry.[288] More importantly, purpose limitation is a key tool to prevent the unexpected aggregation of information into new information about consumers without their knowledge.[289]

Here a reader might wonder. Demanding authorizations from the data subject for each secondary use of information would increase transaction costs, especially given that personal information is valuable when aggregated, and that information processing involves a large number of data subjects. Isn't the purpose limitation principle, 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 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, the author holds the copyright-created right. Using it without her consent is, therefore, swapping the property rule for a liability rule. In purpose limitation, after having collected information under a lawful basis (and potentially compensating the data subject) under a property rule the corporation would hold the right and could therefore do with the right as she pleases. The purpose limitation principle shows that the right was not fully transferred by data subject consent, as data subjects retain rights over that information. Property rules, therefore, would eliminate such protections.

This is not to say that privacy law should be or should resemble intellectual property law more. This has proven incompatible, particularly due to the different aims that intellectual property law and privacy law seek.[290] What this analogy does, rather, is to show that some of the most

---

[288] GDPR, art. 7(4) & Recitals 32, 43. Article 29 Data Protection Working Party, *Guidelines on Consent Under Regulation 2016/679* (Apr, 10 2018) at 5–7.

[289] *See* Nikolaus Forgó, Stefanie Hänold & Benjamin Schütze, *The Principle of Purpose Limitation and Big Data*, in NEW TECHNOLOGY, BIG DATA & LAW 17 (Marcelo Corrales ed., 2017).

[290] Samuelson, *supra* note 75, at 1140–41; Rochelle Cooper Dreyfuss, *Warren & Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8 (1999). *See also* Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L.

protective features of privacy law, such as the purpose limitation principle, are not property-rules-based and, moreover, are potentially incompatible with property rules.

C. Purpose limitation reform

Given what has been argued in this Part about the importance of the purpose limitation principle and how it interacts with property and liability rules in privacy, one can develop reform proposals to make the purpose limitation principle more effective at addressing the moral hazard problem. Under the GDPR, stated purposes must be specific. As Hoofnagle explains, "vague and abstract purposes such as 'promoting consumer satisfaction', 'product development' or 'optimizing services' are prohibited."[291]

Legislative reforms in countries having or seeking GDPR adequacy status could add that the stated purpose must be specific.[292] This is effectively the position under GDPR,[293] but not in all other jurisdictions with adequacy status. In Canada, for example, adding that the stated purpose must be specific would mean modifying Section 4.2.2. of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[294] Currently, in adequacy countries that lack this requirement, stated purposes that are not found in breach of this provision and are

---

& TECH. REV. 220, 222 (2017) ("these enormous data sets have nothing to do with the creative artistic assets that copyright law serves to protect.").

[291] Chris Hoofnagle, Bart Van Der Sloot & Frederik Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means,* 28 INFO. & COMM. TECH. L. 65, 77 (2019) (adding that "A specific purpose exists, for example, when a pizza delivery service asks for the consumer's address to deliver the pizza")

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

[293] Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, EUROPEAN COMMISSION (Apr. 2, 2013), ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; Hoofnagle, Van Der Sloot & Borgesius, *supra* note 228, at 77 (discussing the purpose limitation principle).

[294] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (Can.).

considered sufficiently limited include things like "workforce productivity" or "market research."[295] While current purpose formulations are helpful for organizations, a reframing of purpose limitation with the objective of informing data subjects about the aims of the data collection, processing, and dissemination in an eventual PIPEDA reform would reinforce meaningful data subjects' consent.

Legislators proposing or reviewing privacy legislation (and enforcement authorities such as data protection authorities within the European Union) should establish a more specific standard to determine when use or dissemination constitutes a new purpose, which in turn determines that the new purpose must be communicated to the data subject with a new request for consent.[296]

One way to do this is by implementing a reasonable person standard.[297] Although one could think that technical aspects would be a poor fit for the reasonable person standard, the reasonable person standard would be compatible with a data-subject-focused purpose limitation principle that aims to reduce moral hazard. This standard would ensure that the purpose will be specified to data subjects in clear and understandable terms.[298] The compatibility stems from the fact that this aim stands in contrast to other private law standards in technical contexts, such as standards in professional responsibility, which aim not

---

[295] *See, e.g., PIPEDA Case Summary #2006-351: Use of Personal Information Collected by Global Positioning System Considered,* OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-351/ (last updated Nov. 30, 2006) (finding acceptable the purpose of "managing workforce productivity"). *See generally* MAXIMILIAN VON GRAFENSTEIN, THE PRINCIPLE OF PURPOSE LIMITATION IN DATA PROTECTION LAWS (2018).

[296] Rauhofer, *supra* note 191, at 146–47 (discussing different interpretations of purpose limitation's compatibility rule).

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

[298] Hoofnagle, Van der Sloot, and Borgesius, *supra* note 228, at 77 ("to 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, art. 5(1)(a), recital 39.

to reduce information asymmetries but rather to increase verifiability for improving the determination of liability when set by third parties.[299]

If one cares about reducing moral hazard, in other words, purpose should be specified in writing for data subjects, not for regulators, to increase certainty and foreseeability.

CONCLUSION

Policy, media, and academic proposals to protect privacy with property abound. As seen in this Article when analyzing their specific arguments, these proposals do not propose creating ownership rights; they rather 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 compensation. The first part of this Article is thus a corrective: when people say "property right over data", what they mean is "some kind of right over data, not necessarily a property right, that is protected by a property rule". This means that, if one wants to attack the proposal that "people have a property right over data", as the claim is typically made, our real target must be the claim that "people have some kind of right over data, protected by a property rule".

These rules produce a specific set of problems for privacy. The second part of this Article shows the flaws in data property. that make it inadequate at protecting privacy rights. They leave out important dignitary considerations, they ignore asymmetric information and unequal bargaining power, and they would fail to address the harms produced by

---

[299] *See* Clark C. Havighurst, *Altering the Applicable Standard of Care*, 49 L. & CONTEMP. PROB. 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 any 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).

inferred or aggregated data. These problems indicate that data property bolsters the wrong protection mechanism.

But data property also has a problem that leads it to defeat itself. That is, privacy harm can be produced 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 ex-ante at the moment of collection (or, in property terms, exchange of information for a price), they produce a moral hazard problem: unless otherwise constrained, companies lack incentives to minimize processing and disclosure harms after the exchange has taken place. This means that data property not only arguably aims to achieve the wrong thing, but it is also ineffective at the very thing they try to achieve. If what one cares about is preventing citizens from being harmed, data property risks turning privacy law into over-inclusive and under-inclusive at the same time.

This Article's finding not only provides a normative reason not to implement data property. It also provides insights for privacy reform. Privacy reforms should move in the direction of complementing their property rule elements with liability rules. This Article analyzes 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. 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.

Both of these are possible as directions for judicial interpretation without statutory reform. Regarding the first, this Article's finding shows that there is value in bringing tort law as a compliment to privacy law by complementing our interpretation of privacy statutes as including liability rules as well as property rules. Regarding the second, courts can interpret the specificity of purposes more narrowly, ruling that too-broad purposes breach purpose limitation.

This argument leads to abandoning the idea that property solves control problems in privacy law, and into creating accountability for privacy harm irrespective of whether such harm accrued in compliance with the law. 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 property scrutinizes.