Beyond Data Ownership

Ignacio N. Cofone*

Abstract

This article shows that data ownership proposals, which are increasingly popular, fail to achieve both broad privacy protection and the narrow type of protection that they were designed to achieve: control. Even if property rules proposals seem like they would provide strong protection, they cannot, by themselves, change the vulnerable situation of data subjects meaningfully. The law must instead protect privacy simultaneously by two mechanisms that the Calabresi-Melamed framework calls property and liability rules.

This mixed rule system translates into abandoning the idea that property achieves control over personal information, and into fusing consent requirements in privacy statutes with private rights of action for privacy harm irrespective of whether such harm accrued in compliance with data protection law.

This criticism also informs current doctrinal privacy law discussions that do not use the language of property. Namely: (i) reinforce the purpose limitation principle and (ii) creating private rights of actions to improve privacy law.

Table of Contents

---

* 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, Inge Graef, Claudia Haupt, Chris Howard, Martin Husovec, Shaz Jameson, Mark Verstraete, and Jacob Victor for their helpful comments. The draft also benefited from an internal presentation at Tilburg University. I gratefully acknowledge that an academic visit to develop this research was supported by Microsoft within the research project of the Tilburg Institute for Law, Technology, and Society, 'Conceptualising Shared Control Over Data,' and financial support for research assistance was provided by the Social Sciences and Humanities Research Council of Canada. I also thank Ana Qarri, Vanessa Di Feo, and Martina Kneifel for their research assistance.

I. Introduction

The idea that privacy should be ownership over one's personal data has gained popularity in new legislative proposals, the media, and academic circles. While a broad version of this idea is not new, novel permutations have appeared, for example in pay-for-privacy, the data as labor proposal, and the propertization of data with blockchain.[1]

These proposals contain a conceptual ambiguity that has created a blind spot both in the arguments in their favor and in valid criticisms against them. Proposals for data property or data ownership do not aim to create a different type of right over personal information. Rather, these proposals aim to maximize data subject control over that information by reinforcing consent

[1] See *infra* Section 2.a.

and creating a marketplace for data that is supposed to extract larger ex-ante compensation for it.

In other words, these proposals aim to enhance something that data protection law statutes and regulations have been doing all along: they rely on data subject control to meaningfully protect their privacy. The difference between existing law and these proposals is that they aim to achieve that objective through a "property rule," instead of doing it by mandating and prohibiting specific activities.

Property rules and ownership, which is also called property rights, are conceptually different. Ownership (or a property right) is a type of right while property rules are what stipulates that whatever right they protect can only be given away with consent. Data ownership is not actually about ownership. It is about consent and control. When people refer to data ownership, they mean data protected by a property rule, and not actually ownership rights over data. One can see this from the language used in the literature and the emphasis placed on consent.

This view has severe problems, but those problems are different than the problems it is usually accused of having. 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) protected by a property rule*. And that this view is criticizable on new grounds.

Prior literature has shown how the property paradigm is undesirable because it leaves out important values and dimensions of privacy. Property-type protections and the control rights that they seek will lead to inadequate protection in the long run due to asymmetric bargaining power, data aggregation, and the very limitations of notice and choice that they inevitably inherit.

But these proposals face another key problem. Seeing these proposals for what they are—a defense of transfer rules, not ownership—allows us to also see how this paradigm is counterproductive at achieving the very thing it is designed to achieve: control. Property rules would lead to inadequate and insufficient control because, by lacking incentive-setting to take care ex-post, they generate a moral hazard problem. This means that companies have no incentives to minimize data risk ex-post, thus reducing people's long-term control over their personal data. That moral hazard problem makes the paradigm self-defeating.

Even if property rules proposals seem like they would provide strong protection, they cannot, by themselves, change the vulnerable situation of data subjects. To achieve even the narrow type of privacy that the property paradigm attempts to achieve (i.e. control), the law must instead protect privacy rights with both consent-based rules and after-the-fact accountability mechanisms. Identifying the failures of the data ownership paradigm shows that having such accountability in addition to consent-based rules is a necessary condition for a robust protection mechanism for people's privacy.

This critique does more than defeat the popular data ownership idea. It also informs two current privacy law discussions that do not overtly use the language of property. The first is the importance of reinforcing the controversial purpose limitation principle. The second is establishing private rights of actions to enforce data protection.

Doctrinally, this means the law must keep existing but hotly debated restrictions on the use of data and fuse consent requirements in data protection with new private rights of action. Theoretically, it translates into abandoning the idea that property effectively solves control problems in data protection law, and into creating accountability for privacy harm irrespective of whether such harm accrued in compliance with data protection law. These normative consequences are particularly relevant as the United States considers a federal privacy statute. But, as the article explains, they can also be implemented by the judiciary.

The article proceeds as follows. The next Part provides an overview of the data property and data ownership 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 the property paradigm once properly interpreted. Part V explains why the property paradigm 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 suggests reinforcing the purpose limitation principle to maintain ex-post accountability. Part VII suggests developing a combination of property with liability rules by creating harm-dependent private rights of action. Part VIII concludes.

II. The Popularity of Data Ownership

Data ownership 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. Some 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.

American politics 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.[2] Former Democratic presidential candidate 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.[3] Yang's approach has the particularity that it links ownership with dignity and 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.[4] Yang also started a non-profit organization called *Humanity Forward* that advocates for "data as a property right".[5]

---

[2] *Own Your Own Data Act*, US Bill of Congress, S. 806 116th (introduced March 14, 2019).

[3] Marty Swant, *Andrew Yang Proposes Digital Data Should Be Treated Like A Property Right*, FORBES, 2019, www.forbes.com/sites/martyswant/2019/10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/ (last visited Mar 24, 2020).

[4] Mt. Gox CEO Slams Plaintiff for Adjusting Fraud Allegations Mid-Case, , COINTELEGRAPH , https://cointelegraph.com/news/mt-gox-ceo-slams-plaintiff-for-adjusting-fraud-allegations-mid-case (last visited Jan 1, 2021); 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/ (last visited Jan 1, 2021). See also NBC NEWS, *Andrew Yang Explains Why Digital Data Is Personal Property / NBC News Now* (2019), www.youtube.com/watch?v=tSOf0Eh-4dU (last visited Jan 1, 2021). See also Jaron Lanier & E. Glen Weyl, *A blueprint for a better digital society*, Harv. Bus. Rev. (2018): https://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).

[5] Humanity Forward, HUMANITY FORWARD , https://movehumanityforward.com/ (last visited Jan 1, 2021); Tyler Sonnemaker, *Andrew Yang wants you to make money off your data by making it your personal property*, BUSINESS INSIDER, 2019, www.businessinsider.com/andrew-yang-data-ownership-property-right-policy-2019-11 (last visited Mar 24, 2020).

But European and Canadian politics have also seen versions of this idea. The Canadian Committee on Access to Information, Privacy, and Ethics has recommended that the Canadian government establish rules and guidelines regarding data ownership and data sovereignty with the objective of ending the non-consented collection and use of citizens' personal information.[6] More hesitantly, in 2017 the European Commission launched a consultation group assessing the specific issue of data ownership.[7]

Similar proposals exist in the media. The Financial Times, for example, forcefully argued in 2018 that consumers should be given ownership rights over their personal data.[8] Also in 2018, writer Evgeny Morozov argued in *The Guardian* that big tech, and particularly Facebook, should consider abandoning targeted advertising and move to an ownership-based subscription system with monthly charges.[9] *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."[10]

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.[11] Customer data platform Segment is explicit in stating that

---

[6] Report to the Canadian House of Commons, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, at www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf

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

[8] Editorial, *Digital Privacy Rights Require Data Ownership*, Financial Times (2018), at www.ft.com/content/a00ecf9e-2d03-11e8-a34a-7e7563b0b0f4.

[9] Evgeny Morozov, *After the Facebook scandal, it's time to base the digital economy on public v. private ownership of data*, The Guardian, at www.theguardian.com/technology/2018/mar/31/big-data-lie-exposed-simply-blaming-facebook-wont-fix-reclaim-private-information

[10] The Economist, *We need to own our data as a human right—and be compensated for it* (January 21, 2019) at www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it

[11] Online report, *Who Owns Americans' Personal Information and What is it Worth?* at: https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf

people should own their data.[12] 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."[13] Members of the blockchain community have developed similar proposals, with the idea that blockchain can provide people with ownership over data.[14]

In addition to these normative proposals, one also often encounters the (perhaps mistaken) descriptive statement of "I own my data" in non-technical spaces, from overheard conversations on the bus to Reddit.[15] Current European Commissioner for Competition Margrethe Vestager, for example, discussed

---

[12] Segment, *Why You Should Own Your Data*, at https://segment.com/academy/intro/why-you-should-own-your-data/

[13] Bird & Bird, *Building the European Data Economy – Data Ownership White paper* (January 1, 2017) at 121, at https://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)

[14] See, e.g. David Floyd, *Blockchain Could Make You – Not Equifax –the Owner of Your Data*, at 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*, IBM Developer 2018: https://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…"); Ben Dickson, *How Blockchain Solves the Complicated Data-Ownership Problem*, at: https://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."); Ben Dickson, TechTalks blog 2017: https://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*, 2019: https://medium.com/@markvanrijmenam/how-blockchain-will-give-consumers-ownership-of-their-data-3e90020107e6 ("blockchain is set to change data ownership").

[15] E.g. "This Guy is Selling all his Facebook Data on eBay" thread: 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 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 ?" thread: 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 Own Data Project" thread: www.reddit.com/r/selfhosted/comments/b6o8lu/my_own_your_data_project/

this idea stating 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."[16] Canadian businessman Jim Balsillie, similarly, has argued in Parliament that, due to the effects of the European Union General Data Protection Regulation (GDPR),[17] people have personal ownership of their data, and such data ownership must be woven into a national data strategy.[18]

But these descriptive statements about whether the law as is grants property-akin rights to personal data has found resistance. Importantly, Nadezhda Purtova has shown that introducing property rights in personal data is not consistent with the meaning of property at least under European law.[19] In Teressa Scassa's words, more generally, "the control provided under data protection laws falls short of ownership."[20]

B. Academic 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.[21]

---

[16] Jennifer Barker, *Vestager on the intersection of data and competition*, International Association of Privacy Professionals (October 3, 2018) at https://iapp.org/news/a/vestager-on-the-intersection-of-data-and-competition/

[17] 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).

[18] Standing session at the 42nd Parliament: Standing Committee on Access to Information, Privacy and Ethics (ETHI, Number 106, 1st session, 42nd Parliament (May 10 2018), at www.ourcommons.ca/Content/Committee/421/ETHI/Evidence/EV9861805/ETHIEV106-E.PDF

[19] Nadezda Purtova, *Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation*, 2 EUR. J. LEGAL STUD. 193 (2008). NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (Wolters Kluwer, 2011).

[20] Teresa Scassa, *Data Ownership*, Center for International Governance Innovation Report 187 (September 2018) at 13. See also Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 463 (2018).

[21] *See, e.g.*, Richard Murphy, *Property rights in personal information: An economic defense of privacy*, 84 GEORGETOWN L. J. 2381 (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 clear that ownership rights in personal data become the key instrument in realizing returns on the investment."); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2003).

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.[22] 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.[23] Lawrence Lessig famously promoted the idea of privacy as a form of property rights over data to reinforce people's rights over them.[24]

More recent proposals tend to suggest some altered version of property to obtain a better fit with the goals of privacy. The recent concept of self-sovereign identity, for example, is aimed at users having complete ownership, and therefore control, over their digital identities.[25] 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.[26] Jeffrey Ritter and Anna Mayer suggest regulating data as a new class of property, proposing that regulation of digital information

---

[22] Kenneth Laudon, *Markets and privacy*, 39 COMM ASSOC COMP MACH 92 (1996); Murphy, *supra* note 22; Lawrence Lessig, *The architecture of privacy*, 1 VANDERBILT J. OF ENTRETAINMENT L. AND PRACTICE 56 (1999); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECHNOLOGY L. J. 26 (1996); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 85–90 (1999); Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1–18 (2011); JB Baron, *Property as Control: The Case of Information*, 367 MICHIGAN TELECOMMUNICATIONS AND TECH. L. 367 (2012); Jim Harper, *Perspectives on property rights in data*, AMERICAN ENTERPRISE INSTITUTE - AEI (2019), www.aei.org/technology-and-innovation/perspectives-on-property-rights-in-data/ (last visited Jan 1, 2021).

[23] *See* Prins, *supra* note 22 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.").

[24] LAWRENCE LESSIG, *Privacy as Property*, 69 SOCIAL RESEARCH 247 (2002).

[25] Jeroen van den Hoven et al., *Privacy and Information Technology*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Winter 2019 Edition ed. 2014), https://plato.stanford.edu/archives/win2019/entries/it-privacy/ (last visited Mar 24, 2020).

[26] Leon Trakman, Robert Walters & Bruno Zeller, *Is Privacy and Personal Data Set to Become the New Intellectual Property?*, 50 IIC 937 (2019). See also Will Rinehart, *The Law & Economics of "Owning Your Data"*, AAF , www.americanactionforum.org/insight/law-economics-owning-data/ (last visited Jan 1, 2021).

assets and clear concepts of ownership can be built upon existing legal constructs – in particular, property rules.[27]

The most recent academic proposal along these 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.[28] Data used by companies is produced by humans who are not in 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.[29] In Weil's words, "data as labor treats them [personal data] as user possessions that should primarily benefit their owners."[30] Separately, Weil has argued with Jaron Lanier that, because data is a form of labor, it is labor exploitation to take it without compensation.[31]

III. What it Really Means to Turn Privacy into Property

As the reader may have noticed, all data ownership proposals have something in common: they want people to control their personal information by choosing when to give it away and having the ability to agree on compensation for it. As it turns out, this has nothing to do with ownership, and everything to do with trade.

A. Rights and transfer rules

What we call privacy law and data protection is how the law establishes rights (entitlements) over personal information.[32] Establishing a right and deciding how to protect its transfer are two different things.[33] Besides

---

[27] Jeffrey Ritter and Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 Duke L. & Technology Rev. 221 (2016).
[28] ERIC A. POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY at 209–233 (2018).
[29] *Id.* at 209–233.
[30] Imanol Arrieta-Ibarra et al., *Should We Treat Data as Labor? Moving beyond "Free"*, 108 AEA PAPERS AND PROCEEDINGS 38, 40 (2018).
[31] Jaron Lanier & E. Glen Weyl, *A blueprint for a better digital society*, Harv. Bus. Rev. (2018), https://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).
[32] 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. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1089 (1971).
[33] *Id.* at 1090.

establishing rights, the law establishes a transactional structure for rights.[34] This transactional structure determines under which conditions valid exchanges (transactions) over those rights happen. And the law establishes this structure by placing different transfer rules over rights.[35]

One can distinguish three types of transfer rules: property rules, liability rules, and inalienability rules.[36] Rights protected by a property rule can only be transferred with the title-holder's consent and in exchange for a price determined through bargaining.[37] Examples of these are everyday contracts. Those protected by a liability rule, on the other hand, are transferred without the title-holder's consent and in exchange for a judicially determined price.[38] Liability rules are used mainly due to high transaction costs of ex-ante bargaining—or an actual impossibility.[39] 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.[40] For example, if I agree to sell an organ that agreement will be void. Property rules, liability rules, and inalienability rules thus define the transactional structure of the rights they protect, whichever those rights are.

Property rules are different than ownership—which is confusingly called property rights. 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. On the other hand—in an unfortunate ambiguity—property rules are a transfer rule based on consent that can be used for any type of right.

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

---

[34] Alvin 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 COLUMBIA L. REV. 905 (1985).
[35] Klevorick, *supra* note 35; Klevorick, *supra* note 35.
[36] Calabresi and Melamed, *supra* note 33.
[37] *Id.* at 1106. (stressing the need to enforce voluntary contracts during transfers).
[38] *See, e.g.*, *Id.* at 1107–10. (identifying eminent domain as an example of liability rules).
[39] *See Id.* at 1110. ("efficiency is not the sole ground for employing liability rules rather than property rules").
[40] *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").

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 can hardly be described as ownership. 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.

Thus, one can analyze whether property rules, liability rules, or inalienability rules are the best way to protect the transfer of privacy rights. While inalienability rules are uncommon and their justifications vary,[41] the law often alternates between property and liability rules.[42] If one protects privacy through property rules, the right-holder (data subject) will have the right to decide who can access/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 oneself."[43] 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 mention below, sometimes misconceptualized as property rights or ownership) over information to data subjects has been defended on the grounds that it would force a negotiation that would alter this.[44] Property rules, the argument goes,

---

[41] Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUMBIA L. REV. 931 (1985); Margaret J Radin, *Market-inalienability*, 100 HARVARD L. REV. 1849 (1987); Lee Anne Fennell, *Adjusting Alienability*, 122 HARVARD L. REV. 1403 (2009).

[42] Rose-Ackerman, *supra* note 42; Radin, *supra* note 42; Fennell, *supra* note 42.

[43] Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT (J. LANE, V. STODDEN, S. BENDER, AND H. NISSENBAUM EDS.) 44, 57 (2014).

[44] *See* LESSIG, *supra* note 23; LAWRENCE LESSIG, CODE 2.0 (2006); Julie Cohen, *Examined lives: Informational privacy and the subject as object*, 52 STANFORD L. REV. 1373 (2000).

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).[45] Data subjects, moreover, would be able to extract ex-ante compensation for its release,[46] and they would receive compensation for the expected privacy cost associated with each information disclosure.[47] While this initially *sounds* desirable, there are a number of issues with this approach, described in the next Part.

B. Data ownership 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 treated 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 protected by any transfer rule. Property rights (ownership) are a particular set of rights over a thing. Depending on the theory of property one follows, ownership can be conceptualized as a specific bundle of rights or (in rem) dominium over a thing.[48] 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.[49]

Property-rule protection of personal information is a non-collection default that applies unless consent is given.[50] Property rights often (but not

---

[45] Laudon, *supra* note 23; Murphy, *supra* note 22; Lessig, *supra* note 23; Mell, *supra* note 23; LESSIG, *supra* note 23 at 85–90.

[46] *See* Pamela Samuelson, *Privacy as intellectual property?*, 52 STANFORD 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.").

[47] *See* Prins, *supra* note 22 ("[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.").

[48] Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics Essay*, 111 YALE L.J. 357 (2001); Robert C. Ellickson, *Two Cheers for the Bundle-of-Sticks Metaphor, Three Cheers for Merrill and Smith*, 8 ECON J. WATCH 215 (2011). See also James E. Penner, *The Bundle of Rights Picture of Property* 43:3 UCLA L. Rev. 711 (1995).

[49] See Lisa Austin, *The Public Nature of Private Property* in James Penner and Michael Otsuka (eds) *Property Theory: Legal and Political Perspectives* (2018).

[50] *See* Calabresi and Melamed, *supra* note 33 at 1092 (explaining that "entitlement is protected by a property rule to the extent that someone who wishes to remove the

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 real property) without her consent, and must thus pay her a compensation that will be determined by a judge as a consequence of the forceful transfer of the property right over the object that you breaking it produced.

Most of the policy proposals in favor of treating data ownership or privacy as property rely on 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 real property. In other words, these proposals do not suggest that the right to privacy should be shaped differently—that a bundle of rights akin to real 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.

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.[51] Yang's proposals, similarly, focus on allowing individuals to "share in the economic value generated by their data,"[52] 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;"[53] and control depends on the mechanism through which

---

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").

[51] Report to the Canadian House of Commons: *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, at www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf

[52] Yang, *supra* note 5.

[53] See Mark van Rijmenam, *How Blockchain Will Give Consumers Ownership of their Data*, MEDIUM (2019), https://markvanrijmenam.medium.com/how-blockchain-will-give-consumers-ownership-of-their-data-3e90020107e6 (last visited Jan 1, 2021). See also Ben Dickson, *What's the value of blockchain to consumers?*, TECHTALKS (2017), https://bdtechtalks.com/2017/06/01/whats-the-value-of-blockchain-to-consumers/ (last visited Jan 1, 2021).("Blockchain makes sure that you have full ownership of your data independent of code that runs the application or the companies, servers, service

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. Most of the people who claim that privacy rights should be ownership rights are making a mistake because, without specifying the transfer rule, this identification does not get them the kind of protection that they are after.

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 discussing data ownership do not mean ownership. 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 data subjects' control over their personal information,[54] even though the type of entitlement does little to enhance the person who holds it any 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."[55] 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.

In sum, when people in this space refer to a property right over data, they often mean one protected by a property rule, and not necessarily ownership. One can see from the language used in the literature, and also by the emphasis placed on consent, that the arguments are made with a property rule in mind. 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*. And that this view is criticizable on new

---

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")

[54] van den Hoven et al., *supra* note 26.

[55] Scassa, *supra* note 20, at 14.

grounds. Scholars have correctly argued that the property conception faces important limits. But viewing the property conception for what it is allows us to see that it also defeats itself.

C. Inadequate goal

The property paradigm has centrally been criticized for pursuing the wrong goal. Relatedly, the paradigm has been said to raise constitutional issues, particularly in terms of free speech.[56]

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.[57] 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 fully develop as an autonomous person.[58] Privacy, thus, is much more than 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 when properly read.[59]

Julie Cohen famously argued that property cannot support a broad conception of the protection of privacy.[60] 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.[61]

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

---

[56] Jessica Litman, *Information Privacy/Information Property*, 52 STANFORD L. REV. 1283, 1294 (2000).
[57] Lisa Austin, *Privacy and the Question of Technology*, 22 L. AND PHIL 119 (2003).
[58] Cohen, *supra* note 45 at 1377.; STANLEY BENN, PRIVACY, FREEDOM AND RESPECT FOR PERSONS, IN PRIVACY: NOMOS XIII 8 (Ronald Pennock & John Chapman eds., 1971).
[59] Lisa M. Austin, *Re-reading Westin*, 20 THEORETICAL INQUIRIES IN L. 53 (2019).
[60] Cohen, *supra* note 45 at 1380.
[61] *Id.* at 1384.

IV. Why the Property Conception is Ineffective: Old Reasons Applied to New Ground

Once one understands the property paradigm for what it is, one that focuses on 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 the property paradigm as well. Because of its focus on trade, data ownership creates three structural problems in the protection of privacy rights. First, it inherits the failings of notice and choice. Second, and relatedly, it becomes ineffective at protecting privacy due to unequal bargaining positions. Third, it under-protects personal information obtained through data aggregation.

A. The failings of notice and choice

I showed above that the property paradigm is less about the type of right and more about transferring it through consent. For that reason, the failings of the notice and choice paradigm also translate into the property paradigm. Although this article is not about the benefits and limits of consent in privacy, for that reason, it is helpful to briefly review these criticisms to provide a complete picture of criticisms that are applicable to the property paradigm.

It has been said that "big data extinguishes what little hope remains for the notice and choice regime."[62] While many call for more companies to implement consumer privacy notices as a way to increase transparency,[63] others suggest that notices are ineffective at increasing consumer awareness of how their personal information is managed, even if they are simplified and

---

[62] Solon Barocas and Helen Nissenbaum, *Computing Ethics Big Data's End Run Around Procedural Privacy Protections*, 57.11 Comm ACM 31 (2014) at https://nissenbaum.tech.cornell.edu/papers/Big%20Datas%20End%20Run%20Around%20Procedural%20Protections.pdf (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")

[63] Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (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 (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 COLUMBIA L. REV. 1701 (1999) (explaining the provision of notices as a common method for regulation in medicine).

even if people read them.[64] Indeed, empirical evidence has shown that simplifying disclosures has no effect on consumer awareness, suggesting that language complexity is not the main driver.[65] 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.[66]

This limitation on the usefulness of notices may be due to information overload.[67] 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?). [68] This mechanism is in line with the problem of data aggregation identified above as one of the main drivers of this difficulty would be anticipating how information aggregates.

Beyond descriptive criticisms about the effectiveness of the notice and choice approach, it has received normative criticisms based on the power dynamic between companies, the State, and individuals.[69] 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

---

[64] Kirsten Martin, *Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online*, 45 J. LEG. STUD. 191 (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* (2009); Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. L.POLICY INF. SOC. 543 (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 (2006) (explaining the limits of a disclosure-based policy generally and suggesting direct conduct regulation through the example of securities).

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

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

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

[68] *Id.*

[69] Lisa M. Austin, *Is Consent the Foundation of Fair Information Practices Canada's Experience under Pipeda*, 56 U. TORONTO L.J. 181 (2006); Lisa M. Austin, *Reviewing Pipeda: Control, Privacy and the Limits of Fair Information Practices*, 44 CAN. BUS. L.J. 21 (2006).

and with whom"[70]). As a consequence, the argument goes, the approach insufficiently addresses legitimate countervailing interests. Sometimes, privacy interests can yield to other interests—such as national security or the containment of a pandemic. The consent-based approach approaches this by formulating exceptions for them—such as public interest exceptions. But the formation of obligations for entities who must obtain consent to collect or process personal information in a way that is context-independent fails to appropriately recognize interests that are not the individual's.[71]

Because property proposals pivot on consent and control, the existing criticisms of the notice and choice system also extend to the reliance on consent by property rules.

B. Unequal bargaining positions

A limitation of the property paradigm 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 questionable to what extent property rules improve data subjects' bargaining position when compared to a no-entitlement situation (that is, a lack of privacy rights).[72] Under a property rule, 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.[73] 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 fully be given freely.[74]

---

[70] Lisa M. Austin, *Enough About Me: Why Privacy is About Power, Not Consent (or Harm)* in Austin Sarat, ed., *A World Without Privacy?: What Can/Should Law Do* (2014) at 8.

[71] Id.

[72] Sarah Spiekermann et al., *The challenges of personal data markets and privacy*, 25 ELECTRON MARKETS 161, 6–7 (2015).

[73] *See* Samuelson, *supra* note 47 at 1162 (describing the contractual elements of this relationship).

[74] Elettra Bietti, *Locked-in Data Production: User Dignity and Capture in the Platform Economy* (draft 2019), available at http://dx.doi.org/10.2139/ssrn.3469819, 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").

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.[75] The privacy self-management model is predicated on the false premise that informed and rational individuals will make appropriate decisions as to the use and collection of their personal data.[76] 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.[77] Data subjects lack technical knowledge necessary to sufficiently understand terms and conditions.[78] Moreover, understanding them, let along bargaining over them, would take an enormous amount of time.[79] 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.[80]

In addition, it is difficult for the average data subject to properly assess the risks of disclosing her personal information.[81] Data subjects face difficulties in assessing the risks of disclosing because they do not always know how their data *will* be used and what *can* be done with it.[82] Some also argue that data processors even have economic incentives to mislead data subjects, which adds to the problem.[83] "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

---

[75] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2012).
[76] *Id.*
[77] Schwartz, *supra* note 22 at 2076.
[78] Nadezhda Purtova, *Property rights in personal data: learning from the American discourse*, 25 COMPUTER L. & SECURITY REV. (2009).
[79] McDonald AM, Cranor LF (2008) The cost of reading privacy policies. I/S: J. of L. and Policy for the Information Society 4: 543
[80] Nadezhda Purtova *Do property rights in personal data make sense after the Big Data turn?* 10.2 J. of L. and Economic Regulation 64 (2017) at 11-13.
[81] *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 47 at 1128, 1145 (noting that commentators think the law should supply corrective measures).
[82] Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471 (2017).
[83] Trakman, Walters, and Zeller, *supra* note 27.

we have provided, how it is used and by whom, and what it's worth."[84] 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.[85] The costs of assessing risks when providing consent are therefore high.[86]

C. Data aggregation

A second problem is that information often not collected directly but 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.

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. However, she would not have ex-ante compensation for the aggregated information, which is more valuable and potentially more harmful.[87]

Taken individually, these data might not even be valuable enough to induce companies and data subjects to bargain over them but,[88] combined, they present high costs to users.[89] And the way that information aggregates, as well as how high these costs are, are extremely difficult for data subjects to estimate.[90] People lack protection for the risks of disclosing personal data if

---

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

[85] Christine S Wilson, *A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation*, Remarks delivered at the Future of Privacy Forum (6 February 2020), online (pdf): <ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf>.

[86] Samuelson, *supra* note 47. (adding that while most objects that are sold can be replaced, one cannot replace personal data once it is disclosed).

[87] Barocas and Nissenbaum, *supra* note 44; Solove, *supra* note 76 at 1889–991.

[88] *See, e.g.*, Emily Steel, *How much is your personal data worth?*, FINANCIAL TIMES, 2013, https://ig.ft.com/how-much-is-your-personal-data-worth/ (last visited Mar 16, 2020); Ignacio N. Cofone, *Why paying for Facebook won't fix your privacy*, VENTUREBEAT, 2018, https://venturebeat.com/2018/04/17/why-paying-facebook-wont-fix-your-privacy/ (last visited Mar 16, 2020).

[89] Cofone and Robertson, *supra* note 83.

[90] *Id.*

they are given small compensations for each disclosure while they face high expected harms for them in aggregation.[91]

Another extension is that much of the information about one, and therefore one's lack of privacy, is inferred not only from information that one releases but at least partially from information provided by or taken from others.[92] Data about different people are frequently combined.[93] That has led some to consider that personal data is a public good.[94] Consent of any person becomes irrelevant as one aggregates people to the dataset and infers, at least probabilistically, personal information about each person based on the information disclosed by others.[95]

An extension of this problem is the under-protection of anonymized data.[96] Privacy statutes do not protect data without identifiers. But data can always be re-identified.[97] Property rules cannot require compensation upon re-identification because they only exist 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.

But even data that is kept anonymized is informative of individuals in the aggregate. Thus, it can be potentially harmful to individuals because it is informative about groups that they belong to, allowing inferences for members

---

[91] This aggregation problem relates to the dignity-based criticism of data as property. See Bietti, *supra* note 56, 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")

[92] See generally Bietti, *supra* note 56, 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.")

[93] Bietti, *supra* note 56, at 19.

[94] Schwartz, *supra* note 22 at 2084; Ignacio N. Cofone, *The Dynamic Effect of Information Privacy Law*, 18 MINN. J.L. SCI. & TECH. 517, 530–1 (2017).

[95] Barocas and Nissenbaum, *supra* note 44 (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 80 (explaining this in terms of network effects).

[96] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

[97] Arvind Narayanan and Vitaly Shmatikov, *Privacy and Security Myths and Fallacies of "Personally Identifiable Information"*, 53.6 Comm ACM 24 (2010), at www.cs.cornell.edu/~shmat/shmat_cacm10.pdf

of such groups.[98] 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.[99]

A related issue to the informativeness of our information about other people is that the rights themselves are difficult to allocate appropriately as several data subjects may have a claim over a single piece of information.[100]

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.[101] 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.[102] These can be as simple as a group picture.

Data, in other words, is much about inferences.[103] 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.[104]

In sum, property rules do not protect against data aggregation. That is, they do not provide control over information that is created by assembling

---

[98] LINNET TAYLOR, LUCIANO FLORIDI, BART VAN DER SLOOT (EDS.), GROUP PRIVACY (2017) (explaining that anonymized data is informative of preferences, behavior, population mobility, urban dynamics, among others).
[99] Schwartz, *supra* note 22 at 2084; Purtova, *supra* note 79 at 519; Spiekermann et al., *supra* note 73 at 5.
[100] Spiekermann et al., *supra* note 73 at 7.
[101] Eric Posner and E. Glen Weyl, *Radical Markets* (2018) at 205-249.
[102] Bietti, supra note 56, at 19.
[103] Cofone and Robertson, *supra* note 83.
[104] Barocas and Nissenbaum, *supra* note 44.

previously collected information. However, aggregated data is at least equally harmful, and arguably equally worthy of protection, than shared data.

* * *

Consent-for-use is the system that we already have for privacy, and privacy scholars have shown that it does not work. Proposals to give people ownership over their data would thus do nothing to 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 exactly this. They consent to these uses in the terms of service for sites like Facebook. Thus, the ineffectiveness of the data ownership model is not just a theoretical failure of bargaining, but one that is actualized.

V. Why the Property Conception is Self-defeating

In addition to these problems, usually raised for other issues, which show that the property proposal would not change the situation of data subjects significantly, data ownership contains a fatal flaw. This flaw is that it introduces a moral hazard problem. This is a qualitatively different problem than the objections presented above. In contrast to the prevailing criticisms, which show how the property conception may be trying to achieve the wrong goal, the moral hazard problem means that the property conception is counterproductive at doing the very thing it tries to do: protect privacy by increasing control.

A. Moral hazard in privacy law

Moral hazard takes place when someone (in this case, a company that collects or processes personal data) has incentives to increase risk because such person does not bear the full cost of such risk increase.[105]

A common type of moral hazard is 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).[106] 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

---

[105] Paul Milgrom and John Roberts, *Moral Hazard and Performance Incentives*, in Economics, Organization and Management (1992) at 166-170, 179, 185-190

[106] John Armour et al, *Agency Problems and Legal Strategies* in Reinier Kraakman et al, The Anatomy of Corporate Law: A Comparative and Functional Approach (2017) at 29–45.

but not in the best interest of the principal (which economists call expropriate).[107]

Moral hazards are what economists call an ex-post information asymmetry problem: it happens after the interaction. If parties to the agreement could know and verify the agent's risk-taking behavior after the agreement, they could try to add a contractual clause that internalize the risk. But they cannot. Because those parties do not know when the agent engages in risky behavior, the agent has incentives to do so.

This moral hazard problem materializes in the relationship between data subjects and data controllers if the sole mechanism to transmit the rights over information processing is data subject consent, as it would be under property rules. Once information is collected, under a sole-consent rule the data collector has full control over the information. The data, however, continues to affect the data subject's interests and wellbeing.

Data controllers 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 (slack). The cost of such safeguards is borne by data controllers, while the benefits are borne by data subjects, so there is no economic reason for data controllers to have these safeguards other than compliance with regulations or a tenuous benefit over competitors from a marketing standpoint.[108]

Second, they have incentives to over-process information, creating less tangible risk (expropriate). In the same way that the cost of safeguards is borne by data controllers 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 data controllers, leading to too much 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 property cannot guarantee this.

---

[107] Id.

[108] Data controllers, in other words, may have incentives to provide baseline safeguards for information only when they are known as entities interacting with data subjects who would react to the practice so that, if they do not provide adequate safeguards, then it may be harder for them to gain consent in later cases or from data subjects. In that case, the costs of inadequate security would not be entirely borne on data subjects but there would be some weak consequences for controllers too.

B. Making market failures worse

This market failure already exists in an ameliorated way under current data protection regimes. But it would be aggravated if we relied on property rules to grant 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.

This market failure would take place and would defeat any permutation of property rules 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 a property rules regime 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. The price increase would reduce the demand for such information in equilibrium, which would reduce the supply of information to meet that demand.[109] This moral hazard problem would, in turn, make the market unravel. This, of course, does not happen, 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.[110] 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 that companies lack incentives to incorporate under a property regime, are different. These

---

[109] *See* Murphy, *supra* note 22 at 2385 (describing the "efficiency loss" associated with inhibited information disclosure due to higher cost).

[110] Ignacio Cofone, *The Value of Privacy: Keeping the Money where the Mouth is*, Proceedings of the Workshop on the Economics of Information Security (2015).

measures could be cybersecurity protections to prevent data breaches. Arguably, cybersecurity regulations mandate these protections precisely because consent-based data protection 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 companies have incentives to engage in the socially inefficient behavior because they can externalize this cost.

C. Transaction costs in privacy law

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 before the moral hazard market failure, for a property rule to work data subjects have to know the expected cost of their information to ask for an equivalent price and be compensated ex-ante.[111]

Privacy harms involve several potential parties who are unidentifiable ahead of time, many of whom only come into contact with the data ex-post.[112] 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.

In sum, data, unlike other things that are typically property, have the capacity to affect the data subject's interest after transfer. Property rules can protect from wrongful collection, but not from wrongful use or wrongful

---

[111] Cofone, *supra* note 95.

[112] 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").

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. Normative Consequences: Purpose Limitation

The purpose limitation principle is one of the key provisions of the GDPR and privacy statutes of countries that have or seek GDPR adequacy status. But purpose limitation takes the legal regime away from property rules significantly. Coincidentally, purpose limitation is also is an indirect way to reduce the moral hazard problem. The usefulness of the purpose limitation principle is illustrative of why data ownership proposals 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 purpose limitation principle is established in the GDPR by Articles 5(1) and 6(4).[113] 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.[114] Further data processing is justified only on a new lawful basis for processing; that is, one of the legal grounds required to authorize the initial processing.[115] The prior 1995 Directive[116] also included a compatibility requirement,[117] but requirement this was removed later on when giving further precision to the 1995 Directive.[118]

---

[113] Article 6(4), states "*Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure.*"

[114] See Article 6(1)(a) to (e) GDPR.

[115] 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 INTERNATIONAL REV L. COMP & TECH 144 (2014).

[116] *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) (EC).

[117] *General Data Protection Regulation*, EU 2018, c C-2, s 6(1)(b): "Member States all provide that personal data must be: […] b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards".

[118] Moreover, under the current provision, the controller has significant leeway to apply the subjective compatibility test to further process data in Article 6(4)

Indeed, one of the key obstacles to obtaining facile consent that does not constitute meaningful consent is the importance of identified purposes.[119] 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.[120] In 2014, it asked an organization to 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.[121]

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,[122] making it more difficult to impose any restrictions ex-post.[123] 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."[124]

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.[125] In this way, property rules, while they may sound like the most consumer-

---

[119] *See* Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, (November 28 2017), available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051; Office of the Privacy Commissioner of Canada, *Consent and privacy* (May 2016) at www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.

[120] Office of the Privacy Commissioner of Canada, *Public opinion research firm must better inform survey respondents about their personal information use; refrain from collecting full birth dates* (PIPEDA Report of Findings #2011-011).

[121] Office of the Privacy Commissioner of Canada, *Investigation into the personal information handling practices of Ganz Inc.* (PIPEDA Report of Findings #2014-011).

[122] Samuelson, *supra* note 47 at 1138–39 (using the language of property rights and identifying free alienation as a problem of property).

[123] Schwartz, *supra* note 22 at 2090.

[124] Cohen, *supra* note 45 at 1375.

[125] Cofone, *supra* note 95; Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.*, *in* PRIVACY AND SELF REGULATION IN THE INFORMATION AGE (1997) (arguing that if such sales are

protective, actually lower transaction costs for subsequent sales.[126] If companies have to ask data subjects for permission each time such information was traded, transaction costs are higher than with property rules.[127]

Property rules keep transaction costs relatively low precisely because consent needs to be acquired once, and not again for re-use or re-selling of the entitlement that was transferred through consent.[128] 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. By removing this characteristic, the principle generates ex-post accountability that reduces the moral hazard problem. While companies can still use and transfer personal data in risky ways without internalizing such risk, the scope of possibilities becomes more limited.

B. Property and ownership in light of purpose limitation

This last point relates to the stated difference between ownership and property rules. While in ownership over real property, rights are often transferred in their entirety—meaning that the new owner can do with it what she desires[129]— this is not the case for all other ownership-similar types of rights. Ownership-similar rights, such as intellectual property rights, are often protected by a mix of transfer rules.

Intellectual property rights are transferred by a mix of property and liability rules.[130] Take the example of copyright. Regarding the property characteristics of copyright law, authors holding copyright are entitled to

---

made illegal, it would not stop the sales from occurring, but merely cause sales to be more expensive).

[126] Cofone, *supra* note 95.

[127] Swire, *supra* note 126 (stressing the importance of keeping overall prices low).

[128] Cofone, *supra* note 95 at 545.

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

[130] *See* BJ Ard, *More Property Rules than Property: Revisiting the Right to Exclude in IP*, 68 Emory L.J. 685 (2019) (describing the liability rule features of copyright)

exclude others from copying their work.[131] 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,[132] partially alienating their exclusion right, and to request injunctions for the breach of such exclusion.[133] Regarding copyright's liability characteristics, authors face some compulsory licenses and have to accept fair use.[134] While compulsory licenses tend to be specific and limited, fair use is a central trait of copyright law.[135] In other words, purpose limitation allows for ongoing use-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.[136] 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.[137] 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.[138]

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.[139] Compulsory license are usually set at actual damages (or an estimate of how the

---

[131] *See Id.*
[132] *See* CORNISH ET AL., *supra* note 87, at 525–30.
[133] *See* Ard, *supra* note 91 (arguing that copyright statutory damages awards are often high enough to function as property rules).
[134] Trotter Hardy, *Property (and Copyright) in Cyberspace The Law of Cyberspace*, 1996 U. CHI. LEGAL F. 217, 233 (1996).
[135] *See* 17 U.S.C. § 107 (2012). *See also* Pierre Leval, *Toward a fair use standard*, 103 HARVARD L. REV. 1105 (1990); Glynn Lunney, *Fair use and market failure: Sony revisited*, 82 BU L. REV. 975 (2002).
[136] Wendy Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the" Betamax" Case and its Predecessors*, 82 COLUMBIA L. REV. 1600 (1982).
[137] In expectation, they do not reduce the expected number of copies sold—in fact, they may increase sales.
[138] 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 SOCIETY 601 (1983); Richard Posner, *When Is Parody Fair Use?*, 21 J. LEGAL STUD 67 (1992).
[139] 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).

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.[140] 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.

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 data controller 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.[141] What this analogy does, rather, is to show that some of the most protective features of data protection law, such as the purpose limitation principle, are not property rules and are potentially incompatible with property rules.

---

[140] *Id.*

[141] Samuelson, *supra* note 47 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. & TECH. REV. 220–277, 222 (2017) ("these enormous data sets have nothing to do with the creative artistic assets that copyright law serves to protect.").

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 data protection, one could develop reform proposals to make the purpose limitation principle more effective at this task.

Legislative reforms in countries having or seeking a GDPR adequacy decision could add that the stated purpose must be specific. This is effectively the position under GDPR,[142] 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).[143] Currently, in adequacy countries that lack this requirement stated purposes that are not found in breach of this provision and are considered sufficiently limited include things like "commercial purposes" or "market research." 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 subject consent.

Legislators in these countries, and data protection authorities within the European Union, should establish a more specific standard to determine when use or dissemination constitutes a new purpose and must therefore be communicated to the data subject with a new request for consent.

One way to do this is by implementing a reasonable person standard. While some may think that highly technical aspects would be a poor fit for the reasonable person standard, this would on the other hand be compatible with a data-subject-focused purpose limitation principle that aims at reducing the moral hazard market failure. This or other similar standards would aim at ensuring that the purpose will be specified to data subjects in clear and understandable terms,[144] versus other standards prevalent in professional responsibility that are aimed not at reducing information asymmetries but rather at increasing verifiability for improving the determination of liability when set by third parties.

---

[142] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (April 2, 2013), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[143] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.
[144] *Cf.* GDPR Article 5(1)(a) and Recital 39.

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.

D. Normative Consequences: 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 data controller, not the data subject. Liability addresses the moral hazard problem because it causes data controllers 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.

E. The benefit of privacy liability

There is a clear benefit, given what was explained above, of incorporating liability transfer rules in privacy law. 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),[145] reputational damage (e.g. through the dissemination of embarrassing information),[146] physical harm,[147] or discrimination.[148]

Liability rules would in such a way avoid the problems of property rules identified above. Liability rules, precisely, are transactional rules that are

---

[145] 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 (17 July 2018).

[146] See Cofone and Robertson, *supra* note 96 (arguing that privacy harm and reputational harm are conceptually distinct but are both protected by privacy rules).

[147] 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).

[148] 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).

useful when transaction costs are high.[149] The information asymmetry between data subjects and companies operates as transaction costs: as a consequence, data subjects face information acquisition costs that make it difficult for them to reach welfare-enhancing transactions.[150]

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 transactionally 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.[151]

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.[152] In other words, even if the information asymmetry 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.[153] Aggregation, as seen above, presents a problem for any 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

---

[149] *See* Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L. J. 1027, 1036–1072 (1995).
[150] Litman, *supra* note 57.
[151] Calabresi and Melamed, *supra* note 33 at 1110.
[152] *See* Kapczynski, *supra* note 113 at 1009 (explaining that the cost of protecting private information "requires more than relying on formal individual consent").
[153] *See* Calabresi and Melamed, *supra* note 33 at 236 n.3 (stating that, under liability rules, "even if damages are set imprecisely, liability rules can induce beneficial nonconsensual taking").

they would obtain no compensation. Liability rules do not face this problem because they can set ex-post 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.[154]

F. Determining appropriate compensation for privacy

Besides avoiding the problems generated by property rules, liability rules would present an advantage regarding risk aversion. If data subjects are more risk-averse than data controllers, then liability rules could be in the interest of both players in the interaction even besides their ability to solve the moral hazard problem.[155]

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 according to the amount of harm when it happens as opposed to the expected harm whether it happens or not, would therefore be more valuable for data subjects than ex-ante compensation.

---

[154] 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.

[155] *See* Calabresi and Melamed, *supra* note 33 at 1106 (explaining that risk may be reduced from a liability theory because a collective determination of value leads to quick and efficient transactions).

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.

After determining through what mechanism the right is transferred and how to define compensation for it under liability rules, the next question concerns the amount of compensation and whether it is always provided. That is, one can ask 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). The main benefit of negligence is that it induces an appropriate level of care from the victim and tortfeasor, while the main benefit of strict liability is that it induces an appropriate level of both care and activity by the tortfeasor.[156] Negligence usually fails at inducing appropriate levels of activity and strict liability usually fails at inducing adequate care or activity from the victim.[157] So the question about which rule is most appropriate is often seen as 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).[158]

Unlike most types of accidents, privacy harms are unilateral accidents.[159] This means that the potential tortfeasors (data collectors and data processors) control the probability of an accident (harmful processing or data breach) and the extent of harm in the eventuality of that accident almost

---

[156] STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW (1987).
[157] *Id.*
[158] *Id.*
[159] Cofone and Robertson, *supra* note 96.

exclusively.[160] After data are disclosed, they leave the data subjects' sphere of control, thereby also rendering them unable to control the probability of harm.[161] 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.[162]

In addition, both the level of care and the activity levels of data controllers are relevant for the probability of data harm materializing.[163] The types of processing and level of database security (care level), as well as the amount of processing and number of data transfers (activity levels), directly affect the probability of data subject harm.[164]

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. If harm occurs, there will be an obligation to remedy no matter what happens. 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, would induce an adequate level of care by both parties but not an adequate level of activity. Compared to strict liability, it would lead to care by the victim, but in the case of unilateral accidents that is irrelevant.

Moreover, the application of a negligence standard to databases for personal information leakage has been attacked on the basis that the correct level of due care may be uncertain, leading databases to overinvest in care.[165] Note 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

---

[160] *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").
[161] *See Id.* at 1. ("One faction explains the identity theft as a problem of a lack of control over personal information").
[162] Hoofnagle, *supra* note 161.
[163] *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").
[164] *See* Hoofnagle, *supra* note 161 ("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.").
[165] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 261–8 (2006).

accidents because it would fully internalize the externalities.[166] However, an ambiguous negligence standard would still introduce costly uncertainty. From this perspective, a strict liability rule makes it easier to define expectations than does a property rule. Liability rules are more efficient than property rules, even without prohibitively high transaction costs, when those transaction costs stem mainly from imperfect information.[167]

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.

G. 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. But it has not yet explored how this combination should be realized. 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 *California Consumer Privacy Act* (CCPA). But it could also be achieved without a legislative process by expanding the privacy tort to complement current data protection measures. 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. Second, by interpreting that privacy statutes such as the CCPA 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. Traffic law authorities, similarly, sanction individuals for driving with a

---

[166] *See* Hoofnagle, *supra* note 161 at 32–35 (suggesting strict liability for identity theft).
[167] *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).

broken light even when they did not get into an accident because of it. 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 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 competition law are complemented in their ex-officio approach to give way for people to act.[168] In both cases, this would complement statutes that are focused on prohibited behavior with private law lawsuits focused on harmed individuals.[169]

H. Control does not avoid harm

Privacy torts in and of themselves are also not new. 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.[170]

The internet reduced the costs of surveilling people and it allowed for aggregating personal data to create new data, thereby introducing a host of new privacy harms. When a website makes a ghost profile with someone's name on it but they lack evidence of reputational damage, for example, courts are unsure of whether to grant them remedy.[171] When a credit bureau is hacked but victims lack evidence that this has caused them financial damage, courts are unsure of whether to grant them remedy.[172] Because these harms have become more difficult to identify and repair, privacy interests were moved from being protected by private law through torts to being protected by

---

[168] Kai Huschelrath & Sebastian Peyer, *Public and Private Enforcement of Competition Law: A Differentiated Approach*, 36 WORLD COMPETITION 585 (2013).

[169] 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.

[170] 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).

[171] See, e.g., Spokeo, Inc. v. Robins, 578 U.S. ___ (2016).

[172] Editorial, *The Unfinished Business of the Equifax Hack*, BLOOMBERG (January 29, 2019), www.bloomberg.com/opinion/articles/2019-01-29/equifax-hack-remains-unfinished-business (last visited Mar 24, 2020).

ex-ante regulation. This solution avoids the problem of identifying privacy harms because, by moving towards a control paradigm, it identifies harm with regulated conduct: it is not about whether someone was harmed (because that is problematic to identify), but about whether someone used personal information without a legitimate basis for processing.

Some of the most paradigmatic cases in data protection law, such as *Lindqvist*, indirectly illustrate this dynamic.[173] The case was about Bodil Lindqvist, a maintenance worker and catechist at a parish in a small Swiss town. Lindqvist built a website that allowed parishioners to know what was going on in the parish and helped people seeking confirmation to find the information they needed to meet. The website had basic information about members of the parish, such as their hobbies, and let parishioners know that the priest's availability would be limited as he had injured his foot. This would come to be a mistake on Bodil Lindqvist's part. When this website came to the attention of the Swiss public prosecutor, Bodil Lindqvist would learn that she had breached Swiss and European Union Law by processing people's personal information without their consent. What is worse, she had processed sensitive, medical data (a broken foot). For the oversight, she stood to face hefty fines and three different criminal charges.

Privacy scholars often remember this case as an unequivocal success because it was the case where the European Court of Justice first acknowledged Europeans' right to privacy in data protection. It gave teeth to the 1995 Directive, which in turn lay the groundwork for the GDPR, and it came to be cited in other landmark data protection cases like *Google Spain*. But what we often forget is that the case came at a hefty price. It came at the price of a citizen of modest means who had good intentions (communicating with the parish, not profiting from others' data) facing criminal sanctions that she did not understand and many would find disproportionate. Beyond that, it came at the price of solving ex-officio a problem that, arguably, in this concrete case, no one had.

This, as mentioned above, is not uncommon for bodies of the law that move an issue away from tort law into administrative law. The problem with doing so in privacy is that, like in the early days of environmental law (before environmental class actions) and competition law (before private enforcement), victims in this paradigm can easily move to the background: victims can complain to their data protection authority about having suffered harm, but,

---

[173] *Lindqvist v Åklagarkammaren i Jönköpin,* C-101/01, [2003] ECLI:EU:C:2003:596

unless there are private rights of action to accompany public enforcement, whether and how the authorities investigate and sanction is their prerogative. Moreover, if they do investigate, and companies indeed complied with the regulation (they obtained consent), victims have no recourse even when harm has occurred.[174]

Property is not only often an ineffective protection mechanism. Property is also 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?

Privacy statutes such as the CCPA and GDPR largely measure 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).[175] While this paradigm has its benefits,[176] 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.

I. Combining public enforcement with private claims

For these reasons, both public and private enforcement are needed in practice to overcome the information 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.[177]

However, privacy claims in data protection law are currently based on a piecemeal framework that makes it difficult for individuals to bring

---

[174] Ignacio Cofone, *Privacy Law Needs Privacy Harm*, The Hill (August 30, 2019), online: <thehill.com/opinion/cybersecurity/459427-privacy-law-needs-privacy-harm>.
[175] *See* Walker, *supra* note 139.
[176] 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.
[177] See Janet Walker, *Facebook v Douez* and Privacy Class Actions in Ignacio N Cofone, ed, Class Actions in Privacy Law (2020).

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.[178]

While cases based on these regulations are not frequent, some provisions provide space for them and some cases do exist. The GDPR stipulates, in this regard, space for private rights of action. Articles 79 and 82 contemplate the possibility of data subjects initiating actions to obtain redress.[179] However, as of today, there is little precedent on this front and stemming from behavior that breached the GDPR under art. 82(1),[180] with article 79 having surprisingly little traction in courts.[181] 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.[182]

---

[178] Office of the Privacy Commissioner of Canada, *Enforcement of PIPEDA* (April 4, 2020), at www.priv.gc.ca/biens-assets/compliance-framework/en/index

[179] Gabriela Zanfir-Fortuna, *Article 82*, in Christopher Kuner, Lee A Bygrave & Christopher Docksey, eds, *The EU General Data Protection Regulation: A Commentary* (Oxford University Press, 2020).

[180] Article 82(1) GDPR states: "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered".

[181] 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/ (last visited Mar 26, 2020).

[182] Eoin O'Dell, *Compensation for Breach of the General Data Protection Regulation*, 40 DUBLIN U. L.J. 97, 111 (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).

This traction has mainly taken place in The Netherlands,[183] Germany,[184] and Austria.[185] The United Kingdom, similarly, has seen cases in small claims courts based on regulation 22 of the *Privacy and Electronic Communications Regulations 2003* (PECR) when a data controller acts in breach of the regulation, particularly when collecting information absent a lawful basis for processing.[186] Ultimately, Article 82(1) offers an ambiguous statement of claim for compensation that contributes to confusion when implemented by national courts.[187]

Some other consumer privacy statutes in the United States also give rise to direct private rights of action. Some examples are Washington D.C.'s

---

[183] See, e.g., Overijssel District Court (Rechtbank Overijssel), Zwolle, 28 May 2019, AK_18_2047 (Netherlands), online: < uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2019:1827>; Amsterdam District Court (Rechtbank Amsterdam), 02-09-2019 7560515 CV EXPL 19-4611 at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6490; North Holland District Court (Rechtbank Noord-Nederland), 15-01-2020; C / 18 / 189406 / HA ZA 19-6 at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNNE:2020:247. Note that these cases have also relied on Article 6:106 of thefi Dutch Civil Code.

[184] See DLA Piper, *Germany: First Court Decision on Claims for Immaterial Damages under GDPR* (12 December 2018), online (blog): *Privacy Matters* <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 Amtbsgericht Diez, 07-11-2018, 8 C 130/18 at https://openjur.de/u/2116788.html; Landgericht Karlsruhe, 02-08-2019; 8 O 26/19 at https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Karlsruhe&Datum=02.08.2019&Aktenzeichen=8%20O%2026%2F19.

[185] Oberlandesgericht Innsbruck, 13-02-2020, at www.dataprotect.at/2020/03/06/post-schadenersatz/. Note that the Higher Regional Court of Innsbruck reversed the judgment but not due to a disagreement in law about non-material damages but rather about the standard that should be applied for them.

[186] See Lloyd v Google LLC [2019] EWCA Civ 1599 (02 October 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(3) J. of Intellectual Property, Information Technology and E-Commerce L. 271 (2016).

[187] O'Dell, *supra* note 183 at 112.

Use of Consumer Identification Information Act,[188] and Illinois' *Biometric Information Privacy Act*,[189] which famously triggered a lawsuit against Six Flags,[190] and more recently, a class action lawsuit against Clearview AI for building one of the largest facial recognition databases in history.[191] Regarding omnibus statutes, 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,[192] but it lacks private rights of action to enforce most of its elements.[193] The most recent version of Washington's *Privacy Act*, however, does not contemplate a private right of action.[194]

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 amount of 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. The only way to solve the moral hazard problem is to add liability rules to data protection. And to

---

[188] See e.g. *Hancock v. Urban Outfitters, Inc*, 830 F (3d) 511 (DC Cir 2016).
[189] *Biometric Information Privacy Act*, Pub Act No 95-994, 740 ILCS 14/1.
[190] See e.g. *Rosenbach v. Six Flags Entertainment Corp*, 2019 IL 123186.
[191] *David Mutnick v Clearview AI, Inc, Richard Schwartz and Hoan Ton-That*, US District Court for the Northern District of California Case No 1:2020cv00512, online: <scribd.com/document/444154093/gov-uscourts-ilnd-372790-1-0?campaign=VigLink&ad_group=xxc1xx&source=hp_affiliate&medium=affiliate>.
[192] CCPA s 1798.150; CAL. CIV. CODE § 1798.155(a), (b).
[193] Anupam Chandler, Margot Kaminski & William McGeveran, *Catalyzing Privacy Law* [draft 2020] at 21.
[194] US, SB 6281, *An Act Relating to the management and oversight of personal data; adding a new chapter to Title 19 RCW; prescribing penalties; and providing an effective date*, 66th Leg, Reg Sess, WA, 2020 at s 11.

add liability rules to data protection is to create liability for harm created independent of whether it was done in breach of data protection. In other words, it is to internalize the externalities of data protection.

So statutes like the GDPR and CCPA that make private rights of action depend on breach of regulated conduct and agnostic to harm do this exactly wrong. To be effective at protecting consumers, these private rights of action should instead depend on harm.

VII. 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 rather protecting existing privacy rights with what Calabresi and Melamed call property rules.

In other words, data ownership 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 really 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 thus shows the flaws in this latter proposal. Property rules have problems that make them inadequate at protecting privacy rights. They leave out important dignitary considerations, they ignore unequal bargaining power, and they would fail to address the harms produced by inferred or aggregated data. Because they rely on consent as a transfer and pricing mechanism, they inherit the well-known limitations of the notice and choice paradigm. These problems indicate that property rules may be aiming to achieve the wrong thing.

But property rules for privacy also have a problem that leads them to defeat themselves. That is, privacy harms 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 property rules not only arguably aim to achieve the wrong thing, but they are also ineffective at aiming the very thing they try to achieve. If what one cares about is preventing citizens from being harmed, moving towards property rules paradigm risks turning privacy legislation into over-inclusive and under-inclusive at the same time.

This article's finding not only provides a normative reason not to move towards data ownership. It also provides insights for privacy reform. To address the issues with property rules, privacy reforms should move in the direction of complementing existing property rule elements with liability rules. This article analyzes two ways to do this. The first is reinforcing the purpose limitation principle. While purpose limitation improves consent, it ironically contradicts property rules by placing limitations on use and disclosure after the exchange and at the same time betters them by reinforcing meaningful consent. The second 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.

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