

Data Property

James Grimmelman^{*}

Christina Mulligan[†]

In this, the Information Age, people and businesses depend on data. From your family photos to Google's search index, data has become one of society's most important resources. But there is a gaping hole in the law's treatment of data. If someone destroys your car, that is the tort of conversion and the law gives a remedy. But if someone deletes your data, it is far from clear that they have done you a legally actionable wrong. If you are lucky, and the data was stored on your own computer, you may be able to sue them for trespass to a tangible chattel. But property law does not recognize the intangible data itself as a thing that can be impaired or converted, even though it is the data that you care about, and not the medium on which it is stored. It's time to fix that.

This Article proposes, explains, and defends a system of property rights in data. On our theory, a person has possession of data when they control at least one copy of the data. A person who interferes with that possession can be liable, just as they can be liable for interference with possession of real property and tangible personal property. This treatment of data as an intangible thing that is instantiated in tangible copies coheres with the law's treatment of information protected by intellectual property law. But importantly, it does not constitute an expansive new intellectual property right of the sort that scholars have warned against. Instead, a regime of data property fits comfortably into existing personal-property law, restoring a balanced and even treatment of the different kinds of things that matter for people's lives and livelihoods.

^{*} Tessler Family Professor of Digital and Information Law, Cornell Law School and Cornell Tech.

[†] Professor of Law, Brooklyn Law School. The authors served as Advisors to the joint American Law Institute / European Law Institute project on Principles for a Data Economy. While this Article emerged from our conversations about the conceptual issues involved, it reflects our opinions only, and not necessarily the views of the ALI, the ELI, the reporters, or the other participants. We presented earlier versions of this Article to the Nebrooklyn Law and Technology Workshop, the Private Law Workshop at Harvard Law School, the Intellectual Property Scholars Conference, and the NYU Engelberg Tri-State Region IP Workshop, and to faculty workshops at Brooklyn Law School, the University of Colorado Boulder School of Law, the South Texas College of Law, and the University of Minnesota Law School. Our thanks to the organizers and participants, and to Aislinn Black, John Goldberg, Jordan Khorshad, Frank Pasquale, James Penner, Henry Smith, and Bryttni Yi.

TABLE OF CONTENTS

| | |
|--|-----------|
| I. INTRODUCTION..... | 3 |
| II. UNDERSTANDING DATA | 10 |
| A. Data is a Thing..... | 11 |
| B. Property in Intangible Things..... | 14 |
| C. Instances of Data..... | 17 |
| III. THE DATA PROPERTY FRAMEWORK..... | 21 |
| A. Possession and Ownership | 22 |
| B. Rights and Violations..... | 26 |
| C. Data Transactions | 28 |
| D. What Data Property is Not | 30 |
| 1. Property in Personal Information..... | 30 |
| 2. Intellectual Property Rights in Data..... | 33 |
| 3. Property in Files | 35 |
| IV. APPLICATIONS AND REMEDIES | 38 |
| A. Thyroff v. Nationwide: Loss of Access to Data | 38 |
| B. Cloud Storage: Bailments of Data..... | 41 |
| C. Unauthorized Copying of Data..... | 45 |
| D. Sharing Data in Violation of an Agreement | 48 |
| E. Medical Information about Patients | 49 |
| F. Data Taken from Patients' Bodies: Explaining Moore..... | 50 |
| V. CONCLUSION | 52 |

I. INTRODUCTION

In this, the Information Age, people and businesses depend on data. From your family photos to Google's search index, data has become one of society's most important resources. But there is a gaping hole in the law's treatment of data. If someone destroys your car, that is the tort of conversion and the law gives a remedy. But if someone deletes your data, it is far from clear that they have done you a legally actionable wrong. If you are lucky, and the data was stored on your own computer, you may be able to sue them for trespass to a tangible chattel. But property law does not recognize the intangible data itself as a thing that can be impaired or converted, even though it is the data that you care about, and not the medium on which it is stored. It's time to fix that.

Consider the case of sports videographer Kyle Goodwin. He stored back-up copies of his sports footage on the former file-sharing site MegaUpload, which in its heyday hosted 12 billion files for its 100 million users and brought in tens of millions of dollars in revenue.¹ MegaUpload even had its own theme song, featuring its founder and CEO Kim Dotcom and musical superstars including Kanye West, will.i.am, and Macy Gray.² But according to an indictment obtained by the United States Department of Justice, it was also knowingly engaged in massive copyright infringement.³ On January 20, 2012, seventy-six police officers and two helicopters descended on Dotcom's mansion in New Zealand, where they arrested Dotcom and seized assets including a small fleet of luxury cars and

-
1. See Press Release, Electronic Frontier Foundation, *MegaUpload User Asks Court to Return His Video Files* (Mar. 30, 2012), <https://www.eff.org/press/releases/megaupload-user-asks-court-return-his-video-files> (describing Goodwin); John-Michael Bend, *Megaupload is Coming Back and Your Old Account Will Still Work*, DAILYDOT, Jul. 11, 2016, <https://www.dailydot.com/debug/megaupload-back-online/> (noting MegaUpload had 100 million users "before a police raid killed it"); Darren Greenwood, *Megaupload Founder Battles for Bail in NZ*, ZDNET, Jan. 22, 2012, <https://www.zdnet.com/article/megaupload-founder-battles-for-bail-in-nz/> (noting the site hosted 12 billion files).
 2. *MegaUpload Song*, <https://www.youtube.com/watch?v=ooWvn-gBXVc> (Dec. 17, 2011).
 3. Press Release, Department of Justice Office of Public Affairs, *Justice Department Charges Leaders of MegaUpload with Widespread Online Copyright Infringement*, Jan. 19, 2012, <https://www.justice.gov/opa/pr/justice-department-charges-leaders-megaupload-widespread-online-copyright-infringement>. At the time of writing, the indictment is still pending, because founder Kim Dotcom's extradition case from New Zealand is still ongoing.

a life-size statue of the Predator.⁴ Meanwhile, authorities in Hong Kong froze MegaUpload's bank accounts and authorities in the United States seized the megaupload.com domain name and ordered its hosting companies, Carpathia Hosting and Cogent, to disconnect the MegaUpload servers from the Internet.⁵

All of this played out against the backdrop of property rights — rights in the mansion, cars, statue, domain name, and servers.⁶ But MegaUpload's *users* like Kyle Goodwin were in a wholly different situation. When the MegaUpload servers were unplugged, users lost access to the files they had uploaded. To be sure, some of these users were probably happy just to be able to walk away, whistling innocently and doing their best not to look like copyright infringers. But others like Goodwin were meaningfully harmed. Around when MegaUpload's servers were taken offline, Goodwin's hard drive crashed.⁷ When he tried to access his backed-up files on MegaUpload's servers, he discovered they were inaccessible.⁸ The government's seizure of the MegaUpload servers had also effectively seized his videos, leaving him with no way to redownload them and harming his business.

-
4. Jonathan Hutchinson, *Megaupload Founder Goes from Arrest to Cult Hero*, N.Y. TIMES, July 3, 2012, <https://www.nytimes.com/2012/07/04/technology/megaupload-founder-goes-from-arrest-to-cult-hero.html>; Joe Mullin, *Kim Dotcom is totally stoked to get his cars and money back*, ARS TECHNICA, Apr. 16, 2014 (describing Dotcom's efforts to reclaim some of his property and listing items which had been seized).
 5. See Letter from Cindy A. Cohn, Legal Director and General Counsel, Electronic Frontier Foundation, to Jay V. Prabhu, Ass't U.S. Attorney, E.D.Va. (Feb. 1, 2012), available at <https://www.eff.org/document/letter-court> (describing actions against the MegaUpload domain name and involving Carpathia Hosting and Cogent); Andy Maxwell, *Broke Again, Dotcom Asks Hong Kong Court for Millions*, TORRENTFREAK, Dec. 1, 2015, <https://torrentfreak.com/broke-again-dotcom-asks-hong-kong-court-for-millions-151201/> (describing bank accounts seized in Hong Kong).
 6. See, e.g., Mike Masnick, *How the US Government Legally Stole Millions from Kim Dotcom*, TECHDIRT, Mar. 27, 2015, <https://www.techdirt.com/2015/03/27/how-us-government-legally-stole-millions-kim-dotcom/> (describing the civil asset forfeiture lawsuit against Dotcom's assets).
 7. Press Release, *supra* note 1.
 8. *Id.*; Press Release, Electronic Frontier Foundation, EFF Asks Appeals Court to Break Through Five-Year Logjam in Megaupload Case: Lawful Users Still Waiting for Return of Files after Government Seizure (April 24, 2017), <https://www.eff.org/press/releases/eff-asks-appeals-court-break-through-five-year-logjam-megaupload-case>.

Goodwin struggled to get his files back, while the other involved parties pointed fingers at each other. The government maintained that, following a search, they had released the servers back to Carpathia Hosting; Carpathia maintained they could not access the servers' content without MegaUpload; MegaUpload could not pay for the servers without the government releasing some of its assets.⁹ But complicated as the situation was, Goodwin's problem stemmed from one fact — that because he had no recognized property interest in his videos, neither the government nor anyone else had a legal obligation to provide him with access to them again.¹⁰

Goodwin's own copyright in his videos could not help him either, because copyright does not provide the relevant kinds of rights. Copyright law allows a copyright owner to prevent others from reproducing, adapting, publicly distributing, publicly performing, and publicly displaying their work.¹¹ But neither the government nor Carpathia did any of these things. Copyright provides no exclusive right against deletion, much less an affirmative right of access. For users other than Goodwin who lost access to their data, copyright might not have applied anyway. Not every user who is storing valuable files is storing "original works of authorship"¹² protected by copyright. For example, a collection of family genealogical records may consist entirely of uncopyrightable facts,¹³ but it is still of immense personal importance to members of that family.

The legal rules that created Goodwin's situation are untenable given the role data now plays in our lives. Imagine losing access to your photos in iCloud, your business records in Freshbooks, or your shared documents in Google Docs.

-
9. See Brief of Interested Party Kyle Goodwin in Support of Emergency Motion for Protective Order at 2, 5, 12, *United States v. Kim Dotcom*, No. 1:12-cr-00003-LO (E.D. Va. Mar. 30, 2012), available at <https://www.eff.org/document/brief-interested-party-kyle-goodwin>.
 10. For a time following EFF's unsuccessful request to the Fourth Circuit to "break through" the "five-year logjam" in the MegaUpload case, it appears that Carpathia Hosting worked with the Electronic Frontier Foundation to allow MegaUpload users to retrieve their lawful files. See *MegaUpload Data Seizure*, <https://www.eff.org/cases/megaupload-data-seizure>, last visited Aug. 18, 2022 (undated content). Carpathia's "megaretrieval.com" website is no longer active.
 11. 17 U.S.C. § 106.
 12. 17 U.S.C. § 102(a).
 13. *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 344 (1991) ("facts are not copyrightable").

Instantly. Without warning. Permanently. The legal system goes wrong when it treats Kim Dotcom’s Predator statute as property, but not also Kyle Goodwin’s video archive.

Accordingly, this Article argues for recognition of a new kind of property — data property — that would define what it means to have data and protect individuals’ rights to their data, in a manner analogous to protection of tangible, personal property.¹⁴

On our theory, data — all data — can be owned when it is embodied in one or more specific physical objects, which we call *instances*. The owner of the data (Goodwin) is not necessarily the owner of the object (Carpathia Hosting); instead, the owner is the person who has *control over the stored information*.¹⁵ Goodwin had just such control: he could download the data, modify it, or even delete it. Ownership of data does not confer rights over the information in it as such; if someone else had a copy of the videos Goodwin created, they would be free under data property law to do with it as they please.¹⁶ Instead, what ownership of data confers is protection against dispossession of and interference with use of the data.¹⁷

There are both conceptual and practical benefits to analyzing data as

-
14. See William J. Magnuson, *A Unified Theory of Data*, 58 HARV. J. LEG. 23, 60 (2021) (calling for law to define “clear property rights over data”).
 15. Contrast our theory, which is based on control over information, with theories based on creation of information. *E.g.*, Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. J. 220 (2017)
 16. They may, of course, be liable to Goodwin under copyright law for unauthorized reproduction, public distribution, and public performances. See 17 U.S.C. § 106.
 17. Computer scientists will recognize the similarity between our taxonomy and the “CIA” triad of confidentiality, integrity, and availability. See, *e.g.*, MATT BISHOP, *COMPUTER SECURITY: ART AND SCIENCE* 3 (2d ed. 2019) (“Computer security rests on confidentiality, integrity, and availability.”); WILLIAM STALLINGS AND LAWRIE BROWN, *COMPUTER SECURITY: PRINCIPLES AND PRACTICE* 13 (3rd ed. 2015) (discussing triad). *Cf.* 44 U.S.C. § 3542(b)(1) (defining “information security” in terms of the triad); 45 C.F.R. § 164.306(a)(1) (requiring that HIPAA covered entities ensure the triad for the data they are responsible for); COMPUTER SECURITY DIVISION, NATIONAL TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS (FIPS-199)* (2004) (using the triad to specify security requirements for government data); We believe the resemblance arises because both lawyers and security experts have independently converged on the same set of values worth protecting.

property. Conceptually, it brings clarity and order to a topic that has generated enormous controversy and confusion. It allows the wholesale deployment of property concepts — possession, title, bailment, license, etc. — to data, rather than requiring the complete reinvention of a new body of law to deal with it. Practically, treating data as property provides a basis for courts and legislatures to extend property rights, torts, and crimes to cover cases like Goodwin’s where existing law leaves harmful gaps.

We recognize that using the term ‘property’ to describe rights in data carries some risk. Rhetorically, using the word ‘property’ is often associated with advocating for broad and expansive rights,¹⁸ and so merely calling our framework “data property” might invite others to advocate for not just the fairly limited personal-property-like rights proposed in this paper, but also for additional

18. For example, using the term ‘property’ can evoke Blackstone’s “despotic dominion” language, John Locke’s Labour-Desert theory, and related ideas that property owner’s rights should be expansive, and are immutable, deserved, and natural. See 2 WILLIAM BLACKSTONE, COMMENTARIES *2 (characterizing property as the “sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe.”); JOHN LOCKE, SECOND TREATISE OF GOVERNMENT (1690). Despite the association of ‘property’ with Blackstone’s despotic dominion language, commentators frequently note that Blackstone’s famous characterization of property was hyperbolic. See Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1362 n.237 (1993) (noting Blackstone “would have admitted that his sentence . . . was hyperbolic. His treatise explicitly discussed, for example, a variety of legal privileges to enter private land without the owner’s consent.”); Shyamkrishna Balganesh, *Debunking Blackstonian Copyright*, 118 YALE L.J. 1126, 1133 (2009) (“By most accounts, when Blackstone defined property as the sole and despotic dominion of its owners, he was far from advocating a form of property absolutism. As legal historians have pointed out, Blackstone’s own description of property doctrine of the time did not reflect this definition. Yet ironically, the Blackstonian idea of property is commonly associated with his definition, rather than his actual description of the subject.”); Richard A. Epstein, *Intellectual Property: Old Boundaries and New Frontiers*, 76 IND. L.J. 803, 805 (2001) (“[T]o look closely at all the forms of property that have existed even before reaching intellectual property is to realize that Blackstone engaged in injudicious overgeneralization”); Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357, 361 (2001) (“Blackstone’s talk about property being a ‘sole and despotic dominion’ was clearly a bit of hyperbole and is inconsistent with the balance of his treatment of property, not to mention with the complexities of modern property law.”)

intellectual-property-like rights that might be unworkable or harmful. The recent debates about the scope of intellectual property rights have been illustrative of this risk. As Julie Cohen notes, most scholars “wanting to resist so-called IP-maximalism have found themselves needing to argue that IP isn’t really property at all,”¹⁹ because the idea of property was so closely associated with expansive rights.

Despite the risk, we still think “data property” is the best label for the rights articulated in this Article, because “data property law” is already here. Courts are *already* hearing cases about property rights in data, but their conclusions and reasoning are inconsistent. For example, in 2007, the New York Court of Appeals held in *Thyroff v. Nationwide Mutual Insurance Company* that purely electronic information could be the subject of conversion.²⁰ Later courts, however, have disagreed about whether to follow *Thyroff*, and if so, how far its logic extends.²¹

-
19. Julie E. Cohen, *Property as Institutions for Resources: Lessons from and for IP*, 94 TEX. L. REV. 1, 8 (2015) (citing NEIL WEINSTOCK NETANEL, *COPYRIGHT’S PARADOX* (2008); Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 132-36 (1999); Mark A. Lemley, *Romantic Authorship and the Rhetoric of Property*, 75 TEX. L. REV. 873, 895-903 (1997) (reviewing JAMES BOYLE, *SHAMANS, SOFTWARE AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY* (1996)); Neil Netanel, *Why Has Copyright Expanded? Analysis and Critique*, in 6 NEW DIRECTIONS IN COPYRIGHT LAW 3, 11-15 (Fiona Macmillan ed., 2008)).
 20. *Thyroff v. Nationwide Mutual Insurance Company*, 864 N.E.2d 1272 (N.Y. 2007).
 21. For example, courts have not agreed on whether conversion of data occurs when the original possessor has not been deprived of access to the data. For example, while a federal district court in Washington declined to dismiss a claim alleging conversion of electronic data, even though the plaintiff was not deprived of the electronic records at issue, in contrast, North Carolina courts have held that conversion of electronic information can only occur when plaintiffs lose access to the information. *Compare Aventa Learning, Inc. v. K12, Inc.*, 830 F.Supp.2d 1083, 1105 (W.D. Wash. 2011); *with Addison Whitney, LLC v. Cashion*, 2017 WL 2506604 at *6-7 (N.C. Super. Ct. June 9, 2017) (expressing that “[t]he better view, and the weight of authority, treats electronic documents as personal property subject to a claim for conversion” but favorably citing North Carolina opinions that hold making copies without depriving plaintiff of possession does not constitute conversion) (citing *RCJJ, LLC v. RCWIL Enters., LLC*, 2016 NCBC LEXIS 46, at *53, 2016 WL 3850403 (N.C. Super. Ct. June 20, 2016) (holding that “making a copy of electronically-stored information which does not deprive the plaintiff of possession or use of information, does not support a claim for conversion”); *RoundPoint Mortg.*, 2016 NCBC LEXIS 17, at *55, 2016 WL 687629 (dismissing conversion claim where plaintiff did “not allege that Defendants copied and then deleted the information so as to deprive

The Supreme Court of Arkansas concluded, “There is simply no reasonable basis for allowing a claim for conversion of paper documents but not for their electronically stored counterparts,”²² and Massachusetts state and federal courts have recognized cases of conversion of purely electronic data.²³ But a federal case interpreting Texas law concluded that New York’s *Thyroff* holding did not apply in Texas,²⁴ courts in Tennessee and Georgia have expressly declined to find that electronic information could be converted,²⁵ and federal district courts applying Wisconsin law declined to recognize a conversion claim for electronic records because “no Wisconsin court has expanded its common law tort of conversion to such property.”²⁶

[plaintiff] from its continued use of the information”); *Horner Int’l Co. v. McKoy*, 2014 NCBC LEXIS 68, at *8, 2014 WL 7591487 (N.C. Super. Ct. Dec. 18, 2014) (dismissing conversion claim where plaintiff did “not allege it was deprived of the information or excluded from use of the information allegedly converted by Defendant”).

22. *Integrated Direct Marketing, LLC v. May*, 2016 Ark. 281, 495 S.W.3d 73, 76 (2016). The court continued, “[E]lectronic data, standing alone and not deemed a trade secret, can be converted if the actions of the defendant are in denial of or inconsistent with the rights of the owner or person entitled to possession.” *Id.*
23. *See Children’s Hospital Corp. v. Cakir*, 2017 WL 4012661 at *4 (D. Mass. Sept. 12, 2017) (holding defendant “liable for conversion because he took the Laptop from Children’s Hospital, deleted data from it, and then returned the Laptop”); *Network Systems Architects Corp. v. Dimitruk*, 23 Mass. L. Rptr. 339, 2007 WL 4442349 at *10 (Mass. Sup. Ct. Dec. 6, 2007).
24. *See Devon Energy Corp. v. Westacott*, 2011 WL 1157334 at *9 (Mar. 24, 2011) (“Courts interpreting Texas law have adhered to the merger rule, requiring a physical object to be the basis for a conversion claim.”).
25. *See, e.g., Wells v. Chattanooga Bakery, Inc.*, 448 S.W.3d 381, 392 (Tenn. Ct. App. 2014) (“Conversion is the wrongful appropriation of another’s tangible property; an action for the conversion of intangible personal property is not recognized in Tennessee.”); *Internal Med. All., LLC v. Budell*, 290 Ga.App. 231, 659 S.E.2d 668, 675 (2008) (“Conversion is not available as a cause of action with regard to intangible property interests that have not been merged into a document.”); *see also see also Thompson v. UBS Financial Services, Inc.*, 443 Md. 47, 58-62 (2015) (in a case involving a life insurance policy, declining to remove “conversion of a document” as an element of conversion of intangible property under Maryland law).
26. *In re Dealer Management Systems Antitrust Litigation*, 362 F.Supp.3d 558, 577 (N.D. Ill. Jan. 25, 2019); *see also Epic Systems Corp. v. Tata Consultancy Services Ltd.*, 2016 WL 4033276 at *27 (W.D. Wisc. July 26, 2016) (“While the court finds the reasoning of [courts recognizing conversion claims in electronic data], there is, at least so far, no support from

Courts hearing these kinds of cases would benefit from the development of a thoughtful and rigorous data property framework. Avoiding the term ‘property’ while articulating concepts like possession and rights violations, when courts are already explicitly grappling with concepts like conversion of data, would confuse matters far more than clarifying them.

This Article will motivate why a system of property in data makes sense and describe how it can work. Part II addresses why data is an appropriate subject of property rights and explains how data differs from other kinds of property, setting the stage for Part III’s specific proposals for how data property rights should be framed. Part IV explains specific applications of data property law.

II. UNDERSTANDING DATA

We start with a bedrock premise of this Article: the recognition that, as used throughout American law and many other jurisdictions, *property is the law of things*.²⁷ For purposes of motivating data property law, we mean a fairly mild version of the statement: that “property law” simply is an umbrella term for laws that set forth rights establishing how people can use and exclude others from using discrete resources, or *things*.²⁸ Although this is the starting point of this Article, we recognize that some thinkers have minimized or dismissed the role of *things* entirely in property law. For example, Wesley Newcomb Hohfeld famously argued that *in rem* “property” rights in a thing could always be decomposed into individual *in personam* rights between people,²⁹ and other legal realists followed his lead in claiming that there are no “things” at the heart of property.³⁰ Later thinkers

Wisconsin courts for such an expansion of this state’s common law — at least, plaintiff has failed to direct the court’s attention to such cases.”).

27. Henry Smith, *Property as the Law of Things*, 125 HARV. L. REV. 1691 (2012).
28. See Thomas W. Merrill, *The Property Strategy*, 160 U. PA. L. REV. 2061, 2062-64 (2012). Merrill notes that, in contrast to the discrete things which can be the subject of property, “[s]ome resources are too abstract to be regarded as discrete, such as ideas or cultural knowledge.” *Id.* at 2064.
29. Wesley N. Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 26 YALE L.J. 710, 743 (1917) (noting that “the supposed single right in rem . . . really involves as many separate and distinct ‘right-duty’ relations as there are persons subject to a duty”).
30. See, e.g., Arthur L. Corbin, *Taxation of Seats on the Stock Exchange*, 31 YALE L.J. 429, 429 (1922) (noting “our concept of property has shifted Property has ceased to describe any res, or object of sense, at all and has become merely a bundle of legal relations—rights, powers, privileges, immunities.”); Felix S. Cohen, *Transcendental Nonsense and the*

argued that the term “property” has no necessary content, so that property law is an infinitely malleable “bundle of sticks.”³¹

While these thinkers provided valuable insights into the potential malleability of property rights, we think J.E. Penner got it right when he observed that even the most committed advocate of the “bundle of sticks” struggles to avoid referring to *the thing* in question when articulating what sticks are and are not in the bundle. As Penner put it, “If there was ever any real possibility that a radical Hohfeldian version of the bundle of rights would serve as a new basis for understanding property, it has not materialized. No one has ever produced a general description of the incidents of property which transcends a reliance, either explicitly or implicitly, on an underlying relation between the property owner and the ‘thing’ he owns.”³² Importantly, the core notion of *thinghood* is separable from the notion that there are limits on the malleability of property. So while this Article builds on the premise that “property is the law of things,” its arguments do not rely on the idea that property rights are immalleable, are natural, or that they necessarily include any particular content.

With our premise in mind — that property is the law of things — we turn to the question of whether data can appropriately be made the subject of property rights, and how its nature informs what kind of rights in data would make sense.

A. Data is a Thing

If “property is the law of things,” then data property law can only cohere if data can be characterized as a *thing*. Put another way, we can only describe how something can or can’t be used, and by whom, if we can conceptualize and articulate what the ‘it’ is that we are talking about. The claim that “data is a thing” is a descriptive claim — it means that data *can* be the subject of property law, not that it should or must be. Importantly, ‘thinghood’ is separate from the rights or obligations that society and law choose to recognize. For example, we might recognize the text of *Dracula*, published in 1897, and *Interview with the Vampire*,

Functional Approach, 35 COLUM. L. REV. 809, 815 (1935).

31. Thomas C. Grey, *The Disintegration of Property*, in PROPERTY: NOMOS XXII 69, 69, 74 (J. Roland Pennock & John W. Chapman eds., 1980); A.M. Honore, *Ownership*, in OXFORD ESSAYS IN JURISPRUDENCE 107, 112-24 (A.G. Guest ed., 1961) (describing various incidents of ownership).

32. J.E. Penner, *The “Bundle of Rights” Picture of Property*, 43 U.C.L.A. L. REV. 711, 733 (1996).

published in 1976, as the same kind of intangible ‘thing,’ but only recognize and enforce legal rights in the latter because of a prudential judgment that older works should be in the public domain and newer works should be protected by copyright. A different legal system might justify recognizing the same rights, or no rights, in both texts. *Thinghood* does not have to determine whether a legal system recognizes property rights in a thing or what the character of those rights are, but *thinghood* is a conceptual prerequisite to being able to recognize certain kinds of rights and obligations in or relating to those things.

Conceiving of data as a thing may initially be challenging. In comparison, understanding chattels as things seems quite easy. It seems that physical objects exist in the world, and they have natural boundaries that distinguish them from each other. The spoon in your coffee exists at a specific place in the world, and it has consistent physical properties like length and mass. Recognizing the spoon as a *thing* appears to be merely a matter of finding these pre-existing objective facts. Moreover, recognizing the spoon as *a* thing which is a distinct thing from the mug also appears to be a matter of finding pre-existing objective facts, because the spoon’s and mug’s physical properties include naturally-occurring boundaries that mark them off from each other.

Data, by contrast, appears to share none of these properties. It most emphatically does not have to exist at one specific place in the world: the same data could be instantiated in numerous diverse and scattered copies; it can be generated by ephemeral processes that have no lasting physical existence at all; it can be stored all together or separated and stored in various places. Compared to physical objects, it seems harder to identify the “natural” boundaries of data, and by extension to identify specific data as some *thing*.

But despite appearances, thinghood is social, not natural. A thing is a thing when people can and do recognize it as a thing. For physical objects, the boundaries of a thing often derive from physical properties, because it is easy for people to observe and agree on those properties. But the thinghood itself inheres in the recognition, because that is what makes it possible for people and social institutions (including the legal system) to talk and reason about discrete things.³³

33. Michael Madison has argued that we can identify “things” in five basic ways: things can be real and independent of the legal system (thing-by-nature), things may be made by their makers (thing-by-design), private bargains (thing-by-contract), via some social process or practice (thing-by-practice), or by law, purely as a function of public policy

As long as data can be *recognized* as a discrete thing, that is enough.³⁴

So people don't need to observe any physical properties of data for them to achieve sufficient consensus on what the data is and where its boundaries lie. Instead, *other* social processes allow us to agree that when we say "the list of residents of Greater Blackacre" or "*Moby Dick*," we are thinking of the same thing.³⁵ The fact that we can't *see* the boundaries of data in the same way we can see a spoon does not present any more of a problem for data than it does for other non-controversial forms of property, such as land. Boundaries — in land, chattels, creative works, and data — are often not naturally visible, but develop because of social practice and use.³⁶ For example, one often cannot *see* the boundaries between two parcels of land, but land surveys, and even social practice, can serve as a basis for creating a shared, even if slightly imperfect, understanding of where Blackacre ends and Whiteacre begins.³⁷

There are at least three useful ways of identifying and demarcating

(thing-by-policy). Michael J. Madison, *Law as Design: Objects, Concepts and Digital Things*, 56 CASE W. RES. L. REV. 381, 386 (2005). We generally agree with Madison that individual people and legal institutions can recognize things via any of these methods, but also understand all five methods as different ways of identifying 'things' via their social relevance. Even apparent things-by-nature are identified with regard to what is useful to talk about; for example, whether it is useful to talk about an individual bee or a hive.

34. See Merrill, *supra* note 28, at 2064 ("The resource must also be discrete. There are many values that are not discrete or 'thing-like' enough to qualify as objects of the property strategy.").
35. We do not take a position on whether the social processes of agreement about the existence and boundaries of things actually *are* linguistic or whether they are merely *like* the process of achieving shared linguistic meaning. For our purposes, the only relevant institution dealing in thinghood is the legal system, which is linguistic through and through.
36. Even when boundaries around 'things' are socially constructed, the ability of those boundaries to change varies. For example, the boundaries of Connecticut, New York, and New Jersey are distinct in a way that three lists of names of people who live in each state are not. The three lists could be just as easily stored together as a list of people who live in the Tri-State Area.
37. Cf. Tun-Jen Chiang, *The Trespass Fallacy in Patent Law*, PRAWFSBLAWG (Aug. 23, 2012), <http://prawfsblawg.blogs.com/prawfsblawg/2012/08/the-trespass-fallacy-in-patent-law.html> ("[B]ased on our everyday experiences, the real property system seems to work reasonably well because we don't feel too uncertain about our real property rights and don't get into too many disputes with our neighbors.").

particular data or information as a thing, each of which can be sufficiently effective. First, one can reference the substance of the data, for example, “the first thousand words of Hamlet.” Second, one can identify the data through reference to the chattel that data is encoded upon: “the information on my flash drive” or “the writing in my diary.” Third and most complicated (though not unintuitive), one can refer to the data through reference to how the data is technically organized on a computer — “the file called *Hamlet*” or “the program called *Excel* installed on my laptop.”

This final example is useful for illustrating how thinghood supervenes on social recognition. A computer’s file management system might identify, for example, a list of phone numbers as one object, a file, even if it is stored in several noncontiguous places on the computer’s hard drive. Due to computer systems’ labeling collections of information as “files,” computer users are encouraged to think about each file as a thing — they can move a file, copy a file, delete a file. While they can alter the contents of the file, *the file* is the unit that users are accustomed to thinking about.

Computer users’ intuition to think about files as objects is not a coincidence — the use of terms like *files* and *folders* encourage computer users to think about data as units of information, like pieces of paper that can be organized in folders in a filing cabinet. As some would say, the design and function of a computer helps *construct* our understanding of files as things. In this case, that construction was largely intentional, to facilitate computer users’ manipulation and use of computer data.

B. Property in Intangible Things

It is worth taking a moment to consider objections to the very idea of property in intangible “things.” Some legal systems, for example, maintain that only physical “things” are property. But their reasoning is unconvincing. German law, for example, defines the scope of property law (*Sachenrecht*) to cover only physical (*körperliche*) objects.³⁸ “The term thus excludes immaterial rights, such as claims or intellectual property rights.”³⁹ The point of the distinction is to draw a sharp distinction between property rights and personal obligations.⁴⁰ It is a product of

38. BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE] § 90.

39. NIGEL FOSTER & SATISH SULE, GERMAN LEGAL SYSTEM AND LAWS 493 (4th ed. 2010).

40. Jurgen Köhler, *Property Law* (Sachenrecht), in INTRODUCTION TO GERMAN LAW 295, 296–97

the conceptual formalism behind the German Civil Code,⁴¹ and it therefore excludes many social things that are unquestionably “property” in the Anglo-American tradition, like corporate shares and contract rights. Other civil-law systems based on the same Roman-law categories are perfectly willing to treat intangible things as property. Under French law, intangible objects can be treated as movable property by action of law (*meubles par détermination de la loi*),⁴² a category that includes “non-material objects such as copyright, patent rights, shares in a company, business goodwill, life annuities (*rentes*), and other rights related to movable property such as pledges and bailees’ interests.”⁴³ The sheer diversity of items in this list shows that there is no serious conceptual or practical barrier to treating intangible “things” as property. Similarly, Louisiana’s civil code distinguishes between corporeal and incorporeal things,⁴⁴ with incorporeal things including “things that have no body, but are comprehended by the understanding, such as the rights of inheritance, servitudes, obligations, and right of intellectual property.”⁴⁵ The differences in their treatment have mainly to do with issues where physicality makes a crucial difference, such as possession⁴⁶ and delivery.⁴⁷ In short, the existence of legal systems that *do* treat intangibles as property disproves the conceptual claim that intangibles *cannot* be property. And some commentators agree that data is propertizable in civil-law systems.⁴⁸

Modern scholars who have considered the question widely agree that intangible “things” can be property.⁴⁹ While a few scholars have questioned this

(Joachim Zekoll & Gerhard Wagner eds., 3rd ed. 2019).

41. See generally JOHN HENRY MERRYMAN & ROGELIO PÉREZ-PERDOMO, *THE CIVIL LAW TRADITION* 63–69 (discussing formalistic “legal science” tradition in German codification).
42. CODE CIVIL [C. CIV.] art. 529.
43. EVA STEINER, *FRENCH LAW: A COMPARATIVE APPROACH* 285 (2018).
44. LA. CIV. CODE. art. 448.
45. *Id.* art. 461. Things “comprehended by the understanding” is not a bad shorthand definition of social things.
46. *Id.* art. 3421 (defining possession of corporeal things).
47. *Id.* art. 2481 (defining delivery of incorporeal things “incorporated into an instrument, such as stocks and bonds”). See generally A.N. YIANNPOLOUS, *I LOUISIANA PRACTICE: CIVIL LAW OF PROPERTY* § 13 (1966) (discussing distinction).
48. Andreas Boerding, Nicolai Culik, Christian Doepke, Thomas Hoeren, Tim Juelicher, Charlotte Roettgen, and Max V. Schoenfeld, *Data Ownership—A Property Rights Approach from a European Perspective*, 11 J. CIV. L. STUD. 323 (2018).
49. E.g., João Marinotti, *Possessing Intangibles*, 116 NW. U. L. REV. 1227, 1256–61 (2022); João

conclusion, their reasoning is instructive. Arianna Pretto-Sakmann starts from the claim that the defining characteristic of property rights (as opposed to personal obligations) is that they necessarily relate to a thing.⁵⁰ In her view, the thing doesn't have to be physical, as long as it can be *located* in physical things.⁵¹ Thus, for example, “[An] idea is not corporeal, but it can be located in all those things which are capable of supporting it. ... [ideas], though incorporeal, are naturally capable of being recognized in particular places.”⁵² Whether or not one agrees with Pretto-Sakmann that locatability is *necessary* to make a thing a proper subject of property, her argument that it is *sufficient* is well-taken. By way of contrast, Ben McFarlane does argue that only physical things can be the subject of “property” rights.⁵³ But this ultimately boils down to a terminological point, not a substantive one. He uses the term “persistent rights” to describe many interests

Marinotti, *Tangibility as Technology*, 37 GA. STATE L. REV. 671, 698–711 (2021); James Y. Stern, *What Is the Right to Exclude and Why Does It Matter?*, in PROPERTY THEORY: LEGAL AND POLITICAL PERSPECTIVES 38, 46 (James Penner & Michael Otsuka eds. 2018); Christopher M. Newman, *Using Things, Defining Property*, in PROPERTY THEORY 69, 89–91; Sjeff van Erp, *Ownership of Data: The Numerus Clausus of Legal Objects*, 6 BRIGHAM-KANNER PROP. RIGHTS CONF. J. 235, 236–41 (2017); James Y. Stern, *The Essential Structure of Property Law*, 115 MICH. L. REV. 1167, 1188–91 (2017); Abraham Bell and Gideon Parchomovsky, *A Theory of Property*, 90 CORNELL L. REV. 531, 577 (2005); LAURA UNDERKUFFLER, THE IDEA OF PROPERTY: ITS MEANING AND POWER 13 (2003); Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 749 (1998); PENNER, *supra* note __, at 118; J.E. Penner, *The “Bundle of Rights” Picture of Property*, 43 UCLA L. REV. 711, 802–7 (1996); Kenneth G.C. Reid, *Obligations and Property: Exploring the Border*, 1997 ACTA JURIDICA 225, 230 (1997); J.W. HARRIS, PROPERTY AND JUSTICE 139 (1996); Honoré, *supra* note __, at 129–34. These scholars all accept the Penner/Smith thesis that property is the law of things and accept that intangibles can be things in the relevant sense. Other scholars, who deny the Penner/Smith thesis, also accept that property law extends to intangibles — for them, the tangible/intangible line is not even an obstacle in the first place. *E.g.*, Christopher Essert, *The Office of Ownership*, 63 U. TORONTO L.J. 418, 435 n.40 (2013) (arguing that treating property in terms of the office of ownership allows a unified treatment of “physical” and “non-physical objects.”)

50. ARIANNA PRETTO-SAKMANN, BOUNDARIES OF PERSONAL PROPERTY: SHARES AND SUB-SHARES 88–93 (2005).

51. *Id.* at 105.

52. *Id.* at 105–06.

53. BEN MCFARLANE, THE STRUCTURE OF PROPERTY LAW 132–33 (2008). *See also* Ben McFarlane & Robert Stevens, *The Nature of Equitable Property*, 4 J. EQUITY 1 (2010).

that are customarily treated as property rights, such as the equitable rights of trustees,⁵⁴ and he treats intellectual property as a “background right” that alienable and good against the world.⁵⁵ Both of these are property in all but name. McFarlane’s analytic distinctions are well-taken, but they show that there are important practical divisions within the category of what we conventionally call “property,” not that intangible things are unpropertizable. Similarly, James Toomey, having developed a theory that things “which cannot in principle be the subject of human dominion cannot be owned,” then immediately qualifies his theory to say that IP is either “related to and drawing on general principles of property law” or an “*approximation* of conceptual ownership.”⁵⁶ Once again, this is property in all but name. If these “general principles” and “approximation” are good enough for IP, they are good enough for data.

C. *Instances of Data*

The critical characteristic of data is that it can be instantiated in numerous physical objects simultaneously: these instances are different tangible objects but they are similar insofar as they each store the same data. Fundamental property concepts — like possession, sale, and conversion — require modifications from existing personal property law to deal effectively with instantiated data.

We can begin to identify what modifications are useful by first understanding how data has historically been indirectly protected in personal property law. Under existing personal property law, when data is instantiated in a physical object — for example, a copy of an obscure public domain novel, printed in a book — the law recognizes the value of the novel (the data) as part of the value of the printed book (the personal property, and the instance).⁵⁷ This way of indirectly recognizing value and property rights in data worked well enough before computers were widespread, because physical objects and the data they contained tended to be inextricably bound up in one another once merged. It is generally not a trivial act to change the information contained in physical chattels

54. MCFARLANE, *supra* note 53, at 23–26.

55. *Id.* at 133–36.

56. James Toomey, *Property’s Boundaries*, VA. L. REV. (forthcoming 2023).

57. “A document is a chattel and is, therefore, itself the subject of property. As such, it may be the subject of a conversion which makes the actor liable . . . for its value. If the document is of peculiar historic, literary, or artistic value, such value may be obtained under ordinary rules of the law of damages.” RESTATEMENT 2D OF TORTS § 242 cmt a.

which are not computers or similarly designed to store changeable information (like an abacus). Records are cut with grooves that produce highly particular sounds. Words are printed on paper with ink. Clay is molded and hardened into particular forms. Even writing on paper with pencil is a nearly permanent act — while we might erase a small mistake, it takes effort and strains the physical integrity of most paper to scrub off all markings on a page and start anew. Painted canvas can be covered, but the original work often remains underneath to be uncovered. Because a merger of chattel and data was historically more permanent, personal property law did not need to develop a mechanism to separate ownership and control of information from ownership and control of the chattel in which the information was instantiated. To have the information was to have the chattel, and vice versa.⁵⁸

Digital storage changed this reality. Now, separating the data contained on a computer's hard drive from its location on the drive is trivial. We move the locations of files without a thought. We rearrange data and defragment our hard drives without even conceiving of what we are doing as moving information from one physical location to another.⁵⁹ Indeed, computers constantly rewrite and rearrange data to improve reliability, security, and efficiency, typically without any action or awareness on the part of users. Because it is nearly free and instantaneous to copy and rearrange data, when computers are involved, we care substantially less about on *what* chattel or what part of a chattel (i.e. where on one's computer storage) information exists, so long as it is persistent and accessible.

Because computer storage disaggregates the relationship between the text of the novel and the book, the value in access to a digital text is severed from the value of whatever part of whatever computer it is recorded on in any given moment. So long as the text is instantiated somewhere a person has access to and control over, that person enjoys the full value of having the work.

It's critical to recognize that the key relationship a person has to data is one

58. Exceptions to this practical reality were exceedingly rare — maybe the closest notion many will have is remembering taking silly putty or light-colored playdough to a newspaper as a child, and effectively “lifting” the ink on the comic's page from the paper to the putty.

59. See Defragmenting Files, <https://docs.microsoft.com/en-us/windows/win32/fileio/defragmenting-files> (Jan. 7, 2021) (describing how a computer moves parts of files to different locations in computer storage when defragmenting).

of access to and control of *the data*, and neither to *particular* copies of the data nor to *all* copies of the data. Intellectual property law has taught us to think about intangible works in terms of rights over *particular copies* (as physical things) and of exclusive rights over *all copies* of works (as information). But neither of these concepts captures the relevant relationship between a person and the data they possess. Someone “has” data when they have a file or program on their computer, in cloud storage, or in another sufficiently convenient format that they have what we would recognize as “control” over it. “Having data” is different than having an exclusive right to data or having a particular copy of data.

For instance, unlike a copyright or patent holder, someone who has a digital copy of *Hamlet* or a phone directory has no particular power to restrict what other people can do with copies of *Hamlet* or the phone book which exist on their own computers, and vice versa. The relationship one has to these digital works is not one of an intellectual-property holder — a person’s interests in the intangible works do not extend to versions of the work they cannot access or control, any more than one of us has claim over another person’s Nike sneakers or *Seinfeld* DVDs just because we went to the mall and purchased some sneakers and DVDs ourselves.

But “having data” is also different than “having a copy of data,” the situation with which intellectual (and chattel) property law’s first sale doctrine concerns itself.⁶⁰ The first sale doctrine recognizes a person’s right to use and distribute a *particular* copy of a work or invention, closely tying any rights to information to the physical thing that encodes it, even when the focus of the socially understood thing is on the information itself. But “having data” concerns

60. Copyright law codifies the first sale doctrine in the copyright statute. See 17 U.S.C. § 109(a) (specifying “the owner of a particular copy or phonorecord lawfully made under this title, . . . is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord”). Copyright cases like *Capitol Records v. ReDigi* suggest that the first sale doctrine of personal property law and non-digital copyright law can apply in a digital context — to *particular* digital copies that are stored in a particular part of a computer’s memory. See *Capitol Records, LLC v. ReDigi Inc.*, 934 F.Supp.2d 640, 654–56 (S.D.N.Y. 2013). In patent law, the first sale doctrine, or doctrine of exhaustion, is judge-made. See Herbert Hovenkamp, *Post-Sale Restraints and Competitive Harm: The First Sale Doctrine in Perspective*, 66 N.Y.U. ANN. SURV. AM. L. 487, 511 (2011); see also *Adams v. Burke*, 84 U.S. (17 Wall.) 453 (1873); *Adams v. Burks*, 1 F. Cas. 100 (C.C.D. Mass. 1871).

being able to access and control the data, not any particular instance. This concept implicitly shows up in everyday speech. For instance, if someone you worked with asked if you had the company's quarterly financial reports, you would not say, "I have a computer that contains the reports" or "I have a flash drive that contains the reports." You would just say "Yes, I have the reports," because what matters is that you have them, that you have access to and control of them, not which copy you have, how many copies you have, or where the copies are. Indeed, it often does not even matter if you have the physical thing the data is encoded on. Your relationship to your employer's reports is effectively identical regardless of whether they are stored on your own computer or on a cloud server.

As the quarterly reports example illustrates, the notion that particular copies are the best unit to conceive of digital "thinghood" fails to capture important social realities. Preoccupation with counting copies may or may not be appropriate for copyright law,⁶¹ but focusing on copies in unprotected data obscures what makes data valuable to someone who has access to it. If you have a copy of *Pride and Prejudice* on your laptop, on a flash drive, and in a cloud server, the relevant fact is that you can read *Pride and Prejudice* and that you can send other people copies of *Pride and Prejudice*, not that you have *three* copies. If you copy-and-paste one copy of *Pride and Prejudice* on your laptop to make an identical copy, you have not increased the value of your *Pride and Prejudice* collection by a third.⁶² The difference between having a single instantiation and twenty instantiations is

61. One of us has written about how misguided copyright law's concern with counting digital copies is. See Christina Mulligan, *Copyright without Copying*, 27 CORNELL J.L. & PUB. POL'Y 469 (2017). And Sara K. Stadler has argued for the elimination of the reproduction right. See Sara K. Stadler, *Copyright as Trade Regulation*, 155 U. PA. L. REV. 899, 899, 928 (2007) ("[C]reators are not entitled to expect the right to exclude others from engaging in acts of private copying . . . which, standing alone, do not serve as market substitutes to any significant extent. . . . [C]opyright owners should not enjoy the reproduction right, but instead should enjoy only the exclusive right of public distribution.").

62. Assuming static market demand, you will increase the value of your *Pride and Prejudice* collection if you print another physical copy when you have a limited number, because the new physical copy is an additional instance of the work that you can sell to another person. However, regardless of whether you have one or ten copies of *Pride and Prejudice* on your laptop, you can just as easily send a new digital copy to another.

trivial; the difference between having none and having one is profound.

Thus, the key relationship between a person and information is a relationship of control over the information itself — that someone can access, use, manipulate, and grant to others access to *some instance* of the information somewhere. The value in digital works, or in digital information, is not in the number of copies of the data you have. Rather, the value exists in having access to and control over the data, and in being able to give access and control to others.⁶³ Individuals can manipulate, use, alter, and delete *instances* of the information — copies that exist in a particular place. However, it is not any particular instance of the information that is important — it is one’s ability to interact with *some instance* of the data.⁶⁴

III. THE DATA PROPERTY FRAMEWORK

Now that we better understand how data functions and what relationships to it are valuable, we can begin to develop a framework for recognizing data property. This Part describes what it means to possess data, to own data, and to violate another’s rights in data.

-
63. This relationship between data and one who is in a position to use it is somewhat evoked in the European concept of data controller in data protection law. See Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR], at art. 4(7) (defining a data ‘controller’ as one who “determines the purposes and means of the processing of personal data”).
64. In this respect, data property is *more* natural than intellectual property. Although intellectual property rights are often grounded on an initial relationship of control at some point in time, many major intellectual property regimes thereafter are inattentive to possession as control. By giving owners legal rights to control uses of information with no particular nexus to instantiations they control, intellectual property regimes move further from the intuitions and social realities that drive people’s thinking about things. This is a substantial part of why they are vulnerable to challenges for interfering with users’ liberty interests and why they invite criticism for overreaching. It is also, we submit, part of why data as property has an unfairly bad reputation. One way of understanding our project is as describing the a more limited and more easily justified regime of rights over information — over instantiated information rather than pure information — that intellectual property’s far-reaching claims have obscured.

A. Possession and Ownership

The paradigm case of possession involves direct physical contact with a tangible object: literally holding a book or an apple in your hands. But it is easy to stretch the paradigm in ways that show that the touchstone of possession is *control*, not physical contact.⁶⁵ If you have a book in the backpack you are wearing, or an apple in your apartment, you have possession of the book and the apple because you can control who has access to them. If you have the keys to your apartment, you have possession, because you can control who is allowed inside.⁶⁶ If you are holding the handset to operate a drone as the drone flies overhead, you still possess the drone, because you can control where it goes. In each case, a person possesses a thing when there is social consensus that the person has control over the thing.

When we turn from physical things to non-physical ones, the crucial question is how to identify the relevant sense of control. For rival intangibles, the U.S. legal system looks to the practicalities of who can make decisions about how they are used.⁶⁷ In *Kremen v. Cohen*, for example, the court held that a domain name was possessed by the person who registered it: “Someone who registers a domain name decides where on the Internet those who invoke that particular name ... are sent. Ownership is exclusive in that the registrant alone makes that decision.”⁶⁸ Similarly, Bitcoin are possessed by the person who knows the private key needed to sign a transaction transferring them.⁶⁹

Possession of data is a little different, because information is non-rival and

65. See RESTATEMENT (FOURTH) OF PROPERTY § 1.1 (Vol. 1) TD No 2 (2021) (“A person has possession of a physical thing if the person has established effective control over that thing and manifests an intent to maintain such control to the exclusion of others.”); *id.* cmt. a (describing ‘possession’ as “a legally significant statement of social fact about the world, in the sense that it describes a perceived relationship between particular actors and particular things” and noting the distinction between possession and having a right to possession”).

66. See RESTATEMENT 2D OF TORTS § 157 (defining a person who is in possession of land as one who “is in occupancy of land with intent to control it”); *id.* at § 216 (defining a person who is in possession of a chattel as “one who has physical control of the chattel with the intent to exercise such control”).

67. See generally Marinotti, *Possessing Intangibles*, *supra* note 49.

68. *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003).

69. A few other examples of rival intangibles include email accounts, corporate shares, taxi medallions, places in line, and debts. These are all socially defined. In some cases (e.g. corporate shares and taxi medallions), that definition rests on a substrate of supporting

non-excludable. The only way to keep exclusionary control over information as such is to never to reveal it to anyone else; three may keep a secret, if two are dead. But if we focus on what it means to be able to *use* data, there is another possibility. To analyze data, or to ponder it, or to enjoy it for its own sake, one thing and one thing only is required: an instance of the data. Once you have that, you have control of the information itself, in the sense that you can do whatever you want with it.

Thus, we define possession of data as *control over an instance of the data*. If you have an accounting file on your hard drive, you possess the data in it. If you have photos stored in the cloud, you possess the data in them. If you have a USB stick with historical weather data, you possess that data. And so on. In each case, you

legal rules. In some cases (e.g., email accounts and domain names), the definition rests on a supporting technical infrastructure. And in some cases (e.g., places in line), the relevant social facts are informal and uncodified. Sometimes there is a single authoritative copy that encodes the intangible (e.g., taxi medallions and the records of the municipal franchising agency). Sometimes there are multiple copies that encode the intangible (e.g., the computers in the worldwide DNS system). (For a brief explanation of the domain name system, see *How the Domain Name System (DNS) Works*, VERISIGN, https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml (last visited Aug. 18, 2022); JAMES GRIMMELMANN, *INTERNET LAW: CASES & PROBLEMS* 36 (2021).) And sometimes (e.g. places in line), there are no such copies at all. Sometimes (e.g., email accounts and taxi medallions) a single party is responsible for the underlying substrate and/or copies but does not control the intangible. Sometimes (e.g., debts and places in line) there is no such party. What these examples have in common, despite these many differences, is rivalry. Only one person can control which computer servers a domain name directs to. Only one person can control who the debtor must repay to be free of the debt. If multiple parties try to exercise control of an intangible with conflicting instructions, one of them must prevail. DNS lookups for domain X will resolve to server A or to server B, not to both at once. The debtor only has to pay one putative creditor, not both. The person with control over the intangible is its possessor. Intangibles are rivalrous because of the social consensus surrounding them. If I make an additional copy of the DNS records, it has no effect on the social consensus about who controls a domain name; my new copy *is not the domain-name system*. If you observe people standing in line and write down who is where, your new copy of the order has no effect on the line-standers' social consensus about who was first; your copy *is not the places in line*. For intangibles, the social reality of thinghood constructs the things in a way that enforces rivalry and recognizes only certain (or no) things as authoritative instantiation.

have the necessary control over the data.

This definition is both intuitive and surprising. It is intuitive in that it tracks ordinary lay usage: a person with a copy of the text of *Pride and Prejudice* on their table “has” *Pride and Prejudice*. It is surprising in that it requires lawyers to unlearn some of the assumptions they took on board in first-year Property. For one thing, possession can be overdetermined. If I have *Pride and Prejudice* on my computer, and then also put it on my tablet, and then back up my computer to the cloud, my possession of the informational thing that is *Pride and Prejudice* is essentially unchanged. I now have control over three instances and not one, but the essential fact — that I can make whatever uses I want of the text — is unchanged. For another thing, possession is nonexclusive. Thousands of users can all have possession of *Pride and Prejudice*. My possession of it and your possession of it are perfectly compatible. But while possession of data is not *exclusive*, it is still *excludable* in the more sense that I can prevent you from using my instances of data. I can choose whether or not to give you access to my computer to copy the text of *Pride and Prejudice*. If I do and you make a copy, I have put you in possession of it, and I cannot typically restrict you from putting others in possession as well by letting them make their own copies. But I need not give you access in the first place. This is how far control of data extends.

Note that a person can be in a position to make some use of information without being in a position to exercise full control over it: a patron attending a movie in a theater does not have control over the film being shown and cannot typically make a new instantiation of the same information. We describe this type of situation, which falls short of control and possession, as having *access* to information. Providing access rather than control is a common strategy adopted by possessors of information when transacting in it. I might, for example, let you read *Pride and Prejudice* on my e-reader: you can flip from one screen to the next, but not extract the text in digital form.

In summary, to possess data is to *have effective control over an instance of the data*. This does not require effective control or property rights over the physical medium on which the data is stored: if you have control over a cloud copy, someone else owns and controls the medium and is merely delegating some of that control to you. (Of course, a possessor of data may own or possess the medium as well, as when I put *Pride and Prejudice* on my computer.) This is how rivalrous intangible property works too: control over the property does not require control over the infrastructure. I can possess the domain name `somerandomsite.net`

without possessing the computers that run the Domain Name System; I can possess a Bitcoin even though no one possesses the blockchain it lives on.

Just as possession can be acquired, it can also be lost. One can cease to be a possessor of data by losing control over one's only remaining instance. This could be deliberate or accidental, self-inflicted or caused by another, rightful or wrongful. When control ceases, so does possession.⁷⁰ But if you have two copies of *Pride and Prejudice* and you delete one of them, you still have possession of *Pride and Prejudice*.

Ownership is legally perfected possession. Once the concept of possession is in place, no further modifications are required to make the concept of ownership work for data property. For example, the Restatement of Torts generally makes a trespasser liable to possessors of chattels, and to those entitled to immediate or future possession of the chattel.⁷¹ The same logic works for possessors of data, and those entitled to immediate or future possession of data. If you delete the data from my computer while putting in a new graphics card, you have wronged me in same way as if you destroy my car while repainting it. Possession is similarly regarded as “good against” one without better title to tangible property, and functions as title against a wrongdoer.⁷² We are inclined to describe this legally-protected possession of data as “ownership” — a concept which, although imprecise even in the context of tangible property law,⁷³

70. This concept of possession as control comes, remarkably enough, from European data protection law's concept of a data controller, where it serves very different purposes (identifying who has data protection obligations to a data subject). See GDPR, *supra* note 63, at art. 4(7). But it is the correct concept for property purposes as well. We noticed this fit when the ALI/ELI project on Principles for the Data Economy borrowed the idea of data controllers and processors. See, e.g., ALI-ELI Principles for a Data Economy, Tentative Draft No. 2, (April 28, 2021), at 6, available at https://www.ali.org/media/filer_public/ff/7c/ff7c5006-058e-4254-885d-b5d5725fd8be/date-economy-td2.pdf (stating in the introductory note, “The central player in all data ecosystems is the controller (often also called the ‘holder’) of data, i.e. the person that is in a position to access the data that decides about the purposes and means of their processing.”).

71. See RESTATEMENT (2D) OF TORTS §§ 218-220.

72. 73 C.J.S. PROPERTY § 52 (2020) (citing *Goss v. Bisset*, 411 S.W.2d 50 (Ky. 1967); *Garlock v. Fulton County*, 116 Pa. Super. 50, 176 A. 38 (1935), and *Thomsen v. State*, 70 Wash. 2d 92, 422 P.2d 824 (1966)).

73. “The term ‘owner’ . . . is not a technical term.” 73 C.J.S. PROPERTY § 39 (citing Pinkerton

captures the idea of holding a legally-protected interest in a thing.

B. Rights and Violations

Property theorists have emphasized different aspects of ownership. For some, the core of a property right is the right to exclude others from using a thing.⁷⁴ For others, it is the owner's own right to use the thing that is paramount.⁷⁵ Others give a longer list of incidents of ownership, and worry less about identifying a single right from which all the others can be derived.⁷⁶ But even among this latter camp, the rights to exclude and to use are often cited as particularly important.⁷⁷ Thus, to flesh out how data property would work in practice, we will describe how the rights to exclude and use should be implemented.

First, data property law should protect against *dispossession*. Owners of other forms of property are protected against dispossession by the torts of conversion (for personal property) and ejectment (for real property). These cause of action lie when another uses the property in a way that completely prevents the owner from making any beneficial use of it. Conversion has been extended to

v. Pritchard, 71 Ariz. 117, 223 P.2d 933 (1950); State v. Mitchell, 150 Me. 396, 113 A.2d 618 (1955); Realty Trust Co. v. Craddock, 131 Tex. 88, 112 S.W.2d 440 (1938)).

74. See Francisco J. Morales, *The Property Matrix*, 161 U. PA. L. REV. 1125, 1130 (“Some property theorists equate property with the right to exclude others from the thing owned.”) (citing Shyamkrishna Balganesh, *Demystifying the Right to Exclude: Of Property, Inviolability, and Automatic Injunctions*, 31 HARV. J.L. & PUB. POL’Y 593, 596 (2008) (“The idea of exclusion, in one form or the other, tends to inform almost any understanding of property.”); Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 730 (1998) (“[T]he right to exclude others is more than just ‘one of the most essential’ constituents of property — it is the sine qua non.”); Henry E. Smith, *Exclusion and Property Rules in the Law of Nuisance*, 90 VA. L. REV. 965, 981 (2004) (“Exclusion is a low-cost, but low-precision, method that relies on rough informational variables like boundaries to define legal entitlements.”)).
75. E.g., Newman, *supra* note 49 (describing a use-focused understanding of property).
76. E.g., A.M. Honore, *Ownership*, in OXFORD ESSAYS IN JURISPRUDENCE 107, 112–24 (A.G. Guest ed., 1961).
77. See, e.g., Eric A. Kades, *Property Rights and Economic Development*, 45 WM. & MARY L. REV. 815, 817–18 (2004) (“Perhaps most famously, property law scholars speak incessantly of the ‘bundle of sticks’ that constitute property: various combinations of the rights to exclude, to use, and to alienate as the three sticks that, tied together, make up the bundle of rights we commonly associate with the word ‘property.’”). We discuss the right to alienate in the next Section.

rival intangibles in a straightforward way: for example, in *Kremen v. Cohen*, the defendant converted a domain name by using a forged letter to transfer the registration from the true owner to himself.⁷⁸

In light of the definition of possession of data, the definition of dispossession is equally simple: it is the *wrongful deprivation of a person's control over all their instances of the data*. When you lose your last instance, you go from being able to use the data to being unable to use it.⁷⁹ Note that it is the loss of control over the data that matters, not interference with the physical medium as such. An owner or possessor can be dispossessed of data without losing the medium (as when a hacker erases a person's hard drive), or when they never had property rights in the medium (as when a hacker erases a person's Google cloud storage). Our definition also requires that the loss of control over *all* instances of the data, because destroying only one copy when the owner has a backup leaves them still able to use the data. The same remedies that apply to personal property should be available: an injunction requiring the defendant to restore plaintiff to possession, and money damages to put the plaintiff in their rightful position.

Not all interferences with property are serious enough to constitute complete dispossession. For personal property, there is trespass to chattels; for real property, there are trespass and nuisance. Similarly, data property should be protected against interference that *impairs a person's ability to use an instance of data*. One form of interference is to delete an instance when the owner still has control over another instance. Forcing me to restore my computer from a Backblaze cloud backup is a serious inconvenience, even if I ultimately don't lose any data. Another form of interference is to prevent a person from using an instance.⁸⁰ Temporarily locking me out of my Google Drive is also a serious inconvenience, particularly if I'm racing to make a deadline. And a third (and in some ways the most insidious) form of interference is to alter an instance of data.⁸¹ Forcing me to go line-by-line through an Excel spreadsheet to make sure each entry is still correct is a special form of torture. Appropriate remedies here are injunctions to cease the interference, and money damages for loss of use (of unavailable data), for diminution in value (of altered data), and for the costs incurred in recovering from

78. *Kremen v. Cohen*, 337 F. 3d 1024 (9th Cir. 2003).

79. In information-security terms, this is a violation of availability.

80. In information-security terms, this is also a violation of availability.

81. In information-security terms, this is a violation of integrity.

the interference.

These concepts can be tricky because people usually access data through instances that exist in particular, physical chattels. Thus, so one must be careful to distinguish between *rights to the data* and *rights to the chattel the data is instantiated in*. For example, if you have data on a computer, and a someone uses the computer without permission to make a copy of the data, we might recognize that the user probably committed computer trespass under the Computer Fraud & Abuse Act and possibly trespass to chattels to the computer; in other words, the user violated rights *in the computer*.

Note that these property rights in data emerge from an owner's control over particular instantiations of the data. This is a crucial distinction between data property and intellectual property: data property rights always have a nexus to one or more particular instantiations, intellectual property does not. Another crucial distinction is that while intellectual property law protects a right to exclude others from using information, it does not guarantee the owner's ability to use the information free from others' interference. This is why the copyrights Kyle Goodwin held in his own videos did not help him re-access his videos after MegaUpload's servers were disconnected; copyright law did not provide him with any affirmative right to use or access his works.⁸² In contrast, data property law does not give a data owner any right to exclude others from using the same data; it does not grant intellectual-property-style *exclusive* rights. Rather, data property law protects an owner's ability to use data that is under their control from interference by others.

C. Data Transactions

Data is valuable, and is the subject of major commercial transactions.⁸³ In this Section, we show how our definitions of data property make it transactable. Consider some of the different ways in which an owner of data — someone who has control over an instance — can deal with it.

A *transfer* of data takes place when a party who possesses the data puts another party in possession. In the language of instances, the controller of an instance uses that control to put another party in control of an instance. Notice that this definition is agnostic as to the mechanism by which the transfer takes

82. See 17 U.S.C. § 106 (setting forth the exclusive rights of copyright).

83. See AMERICAN LAW INSTITUTE, PRINCIPLES FOR A DATA ECONOMY (2021).

place. It could involve the legal transfer of ownership and possession of a physical medium (e.g., I give you a portable hard drive containing data), the transfer of possession but not ownership of a physical medium (I provide you a portable hard drive from which you can copy the data but which you must return to me when you are done), the transfer of ownership of the physical medium without a present change in possession (I transfer title to a hard drive in a data center to which both of us make only remote access), or or neither a transfer of ownership nor of possession of the physical medium (I give you virtual access to a hard drive in a data center that that I am leasing from a hosting provider).⁸⁴ This agnosticism is right. The substance of the transaction is that I am *giving you data*; the particular medium I use to make the transfer is a minor procedural detail.

A more important transactional question is whether a transfer is *exclusive* or *nonexclusive*. In an exclusive transfer, the transferor gives up possession: there was one possessor before, and there is one possessor after. In a nonexclusive transfer, the transferor retains possession; there was one possessor before, but now there are two. Transfers of tangible personal property and rival intangibles are inherently exclusive. But nonexclusive transfers are trivially easy with data, so this is a novel form for property transactions, and a part of the reason why a commercial law of data is necessary.⁸⁵

This distinction shows why the idea of a security interest in data is both plausible and tricky to get right. A security interest in tangible property follows a straightforward logic. If the debtor defaults and the creditor levies on the collateral, two things happen at once: the debtor loses possession and the creditor gains possession, giving the creditor the full value of the collateral. But because data is nonrival and transfers can be nonexclusive, these two halves come part. The creditor who gains control over an instance of data takes possession of it, but if the debtor has another instance squirreled away somewhere, they will *also* still be in possession. For some kinds of data, this could defeat the point of levying on the data in the first place.

Similarly, because transfers of data can be forbidden by contract, difficult

84. Allowing a recipient to create a copy from one's own bears some resemblance to the *profit à prendre* in real property law. See BLACK'S LAW DICTIONARY (11th ed. 2019) (defining "profit à prendre" as a "right or privilege to go on another's land and take away something of value from its soil or from the products of its soil (as by mining, logging, or hunting)").

85. See generally PRINCIPLES FOR A DATA ECONOMY, *supra* note 83.

issues will arise involving downstream transferees. These will raise issues analogous to those for good-faith purchasers, void and voidable transactions, fraud in the inducement versus fraud in the factum, recording acts, and so on. Remedies in cases involving data are likely to be trickier than for other kinds of property: its nonrivalrousness can make “return” of data comparatively less appealing, since all this does is impose a loss on the user without typically restoring anything further to the owner. Instead, restitutionary measures that allow the user to retain data while returning its derived value to the owner may be more useful.

D. What Data Property is Not

Data property is a system of property rights analogous to the kind of rights held in personal, tangible property (like books and filing cabinets) and in rivalrous, intangible property (like bank accounts and domain names). It is not a system of exclusive rights, or intellectual property rights, nor is it a system to empower individuals to have greater control over information about themselves. To emphasize these distinctions, this section explains how data property is different from proposed rights in personal information and in intellectual property rights in data.

I. Property in Personal Information

When privacy scholars talk about data property, they tend to use a meaning different the meaning is used in this Article. By “data,” they mean “*personal data*”: information that is specifically about particular individuals. And by “property” they mean property in information *as such*: an *in rem* right to prevent anyone else from using that information. So, in the context of privacy scholarship, a “data property” regime would be one in which individuals have a property right to keep anyone else from using information about them without their consent.

The starting point for most discussion of this kind of system is that there is already a robust market for personal information. Technology platforms collect vast quantities of data on people, tracking their purchases, movements, and interests, and data brokers offer immense dossiers of such data for sale.⁸⁶ From the

86. See generally BENNETT CYPHERS & GENNIE GEBHART, ELECTRONIC FRONTIER FOUNDATION, *BEHIND THE ONE-WAY MIRROR: A DEEP DIVE INTO THE TECHNOLOGY OF CORPORATE SURVEILLANCE* (Dec. 2, 2019), <https://www.eff.org/document/behind-one-way-mirror->

perspective of these companies, personal information already *is* property; they profit from its free alienability. But the people that information is about are left out entirely; indeed, the system is built on exploiting information about them. United States privacy law is a patchwork and imposes very few limits on the initial collection of personal information.

According to the argument for what Paul Schwartz usefully calls “propertized personal information,” giving individuals property rights over their personal information can serve two goals.⁸⁷ On the one hand, it turns them into market participants, rather than bystanders. Vesting the initial property entitlement in their hands, rather than in the hands of the first company to collect it, allows them to negotiate for better terms, and be properly compensated for giving up that information. On the other hand, turning personal information into property would give them access to the full range of property rights and remedies, allowing them to better protect their privacy interests in the first place by suing companies who trade in it.

Opponents of propertized personal information cite a variety of conceptual and practical obstacles.⁸⁸ Some argue that if the problem is the commodification of personal information, then more property rights make the problem worse, not better.⁸⁹ Others argue that as long as individuals’ property rights in their personal information are alienable, a system of propertized personal information will simply replicate the current dysfunctional one.⁹⁰ And still others fear that a system

deep-dive-technology-corporate-surveillance (explaining how businesses track individuals’ behavior on the Internet); SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* (2019) (describing and critiquing how businesses buy and sell data about their users).

87. Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004). Other notable proponents include LAWRENCE LESSIG, *CODE: AND OTHER LAWS OF CYBERSPACE* 142–63 (1999); Lawrence Lessig, *Privacy as Property*, 69 SOC. RES. 247 (2002); Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631 (2010); Vera Bergelson, *It’s Personal But is It Mine: Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2003).
88. *E.g.*, Jorge Contreras, *The False Promise of Health Data Ownership*, 94 N.Y.U. L. REV. 624 (2019); Jorge Contreras, *Genetic Property*, 105 GEO. L.J. 1 (2016); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); James Toomey, *Property’s Boundaries*, VA. L. REV. (forthcoming 2023).
89. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).
90. Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. 501 (2021); Stacy-Ann Elvy,

of propertized personal information might replace a system in which individuals have too few rights with one in which they have too many, giving them a powerful “right to have the government stop people from speaking about you”⁹¹ — a right over information as such of the sort criticized by IP scholars.⁹² What they have in common is a view that privacy concerns ought to be addressed by a true system of privacy law. Proponents of propertized personal information have responded by calibrating the details of their proposed property regime,⁹³ leading other scholars to question “whether the sophisticated, qualified ownership regimes scholars have propounded are appropriately characterized as ‘property’ at all,”⁹⁴ while other scholars ask whether privacy law might already amount to a kind of “quasi-property.”⁹⁵

In one sense, our proposal for a system of data property is not an intervention in the debate over propertized personal information. It would give individuals no new rights over information about them in the hands of third parties. It would confirm that they have the right not to have their personal data exfiltrated from their computers without their consent, but only as a corollary of the more general proposition that they have the right not to have *any* of their data exfiltrated from their computers without their consent. We propose no new rights in data as such, whether it is personal data or not.

But in another sense, our analysis of data property can provide the legal backdrop against which companies transact in data. The existing market for transactions in personal data is one that functions according to the doctrines of data property — the same doctrines that apply to a market for transactions in any kind of instantiated data. Companies that have possession of data strike deals with each other for access and transfer. They have no rights against others who use

Paying for Privacy and the Personal Data Economy, 117 COLUM. L. REV. 1369 (2017).

91. Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

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

93. Schwartz, *supra* note 87; Steven H. Hazel, *Personal Data as Property*, 70 SYR. L. REV. 1055 (2020).

94. Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMM. & TECH. L. REV. 367 (2012). *See also* Contreras, *False Promise*, *supra* note 88.

95. Lauren Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113 (2016). *See also* Jacob M. Victor, *Comment: The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513 (2013).

their own copies of the same data, only rights against those who commit acts of dispossession, interference, and unauthorized use. From the existence of *this* kind of property right (in instantiated data in general, held by the possessor), it does not necessarily follow, either logically or as a policy matter, that *another* kind of property right (in personal data as such, held by the data subject) is appropriate — nor does it follow that propertized personal information, or laws like the European Union’s General Data Protection Regulation⁹⁶ or the California Consumer Privacy Act,⁹⁷ are inappropriate or unworkable. Indeed, data property law can function just as well in a jurisdiction with extensive protections in personal information as it can with none.

2. Intellectual Property Rights in Data

Intellectual property scholars have also debated a system of property in data. But like privacy scholars, what they mean by ‘property’ is a system of *in rem* rights in information as such, not tied to possession of any particular instantiation.⁹⁸ The difference is that where privacy scholars have in mind a system that allocates property rights in (personal) data to the people the data *is about*, the IP scholars are have in mind a system that allocates property rights in (any kind of) data to the people who *compile* the data. Such a system is best described as one of “intellectual property rights in data.”⁹⁹

The basic argument for intellectual property in data is same as the one for any other kind of intellectual property right: creating proper incentives for creators. Companies invest significant amounts of time, effort, and money in producing valuable collections of data. Some of those collections may be original enough to be protected by copyright as a compilation, but much or all of the data in them is uncopyrightable. In order to realize the value of these collections, their creators must share them with others. But because data is non-excludable, once the collections have been shared at all, without further legal protections, they can be freely copied and shared further, undercutting the market for the data and undermining the incentive to create collections in the first place. Exclusive

96. GDPR, *supra* note 63.

97. CAL. CIV. CODE §§ 1798.100-1798.199 (Deering 2020).

98. *E.g.*, Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1 (2019).

99. J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997).

intellectual property rights over the data would prevent such copying, enabling a market for access to the data, and restoring a sufficient incentive for creators.

This is the approach taken by the EU Database Directive, which creates a *sui generis* database right.¹⁰⁰ The right exists whenever “there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents” of the database.¹⁰¹ It provides an exclusive right against the “extraction and/or re-utilization of the whole or of a substantial part ... of the contents of that database.”¹⁰² The database right is copyright-like: it applies to information, is owned by the party who first holds that information, and it can be transferred and licensed.¹⁰³ One major difference is that copyright is based on originality, while the database right is broader and is based on “substantial investment.”¹⁰⁴ Another is that while copyright protection would be limited to the database itself — its “selection or arrangement”¹⁰⁵ — the database right goes further and protects against “extraction and/or re-utilization” of the data within, even if it is selected and arranged differently. But otherwise, it has the same structure as copyright and other intellectual property laws: *in rem* rights over information itself.

Intellectual property scholars have criticized the Database Directive and similar proposals. Just as the arguments *for* intellectual property rights in data reflect general arguments for broader intellectual property rights, the arguments *against* intellectual property rights in data reflect general arguments for narrower intellectual property rights. Scholars argue that intellectual property rights in data threaten to narrow the public domain, to interfere with downstream research and

100. Directive 96/9/EC of the European Parliament and of the Council of March 11 on the Legal Protection of Databases, 1996 O.J. (L 77) 20 [hereinafter “Database Directive”]. See also P. Bernt Hugenholtz, *Something Completely Different: Europe’s Sui Generis Database Right*, in *THE INTERNET AND THE EMERGING IMPORTANCE OF NEW FORMS OF INTELLECTUAL PROPERTY* 205 (Susy Frankel & Daniel Gervais eds. 2016).

101. *Id.* art. 7(1).

102. *Id.*

103. *Id.* art 7(3).

104. This “sweat of the brow” approach has been decisively rejected in the United States. See *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 352–54 (1991).

105. Database Directive, *supra* note 100, art. 3(1). Cf. 17 U.S.C. § 101 (defining “compilation”); *id.* § 103(b) (defining scope of copyright in a compilation).

creativity, and to restrict competition.¹⁰⁶ Other scholars have suggested ways to recalibrate intellectual property rights in databases in light of those concerns.¹⁰⁷

Once again, however, this is not what we are proposing. This is clearest if we consider how first sale works under the two regimes. Under the Database Directive, as under copyright, someone who lawfully buys a copy of a database receives the right to use and transfer that copy — but not to make new copies.¹⁰⁸ The database owner's rights continue to encumber the data instantiated in that copy. But under a data property system, someone who lawfully buys a copy of a database takes the *data itself*, and not just the physical copy, free and clear. They can make and distribute as many new copies as they want. The database creator's rights are restricted to the copies they continue to control. This is a meaningful right — the buyer of one copy is not free to go and destroy the creator's other copies — but it is emphatically not an intellectual property right in the way that copyright and the *sui generis* database right are.

3. Property in Files

A few scholars have argued that files should be recognized as property. Johan David Michaels and Christopher Millard, for example, argue that information as such cannot be property, because its boundaries are too difficult to discern, and because it is neither excludable nor rivalrous.¹⁰⁹ However, they argue, files do have these qualities and are appropriate subjects of property.¹¹⁰ In their view, “a Bitcoin or a file is a *virtual thing* that can be subject to exclusive control at the logical layer of a computer system.”¹¹¹

106. Reichman & Samuelson, *supra* note 99, at 113–37; Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on the Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 440–46 (1999); Samuel E. Trosow, *Sui Generis Database Legislation: A Critical Analysis*, 7 YALE J.L. & TECH. 534 (2004–05).

107. See, e.g., *Symposium: The Constitutionality of Protecting Factual Compilations*, 28 U. DAYTON L. REV. iss. 2 (2002); Estelle Derclaye & Martin Husovec, *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms*, EUR. INTEL. PROP. REV. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4138436.

108. *Id.* art 7(2)(b).

109. Johan David Michaels & Christopher Millard, *The New Things: Property Rights in Digital Files*, CAMBRIDGE L.J., draft at 5–6 (forthcoming 2022) (near-final version available at <https://doi.org/10.1017/S0008197322000228>).

110. *Id.* at 10–14.

111. *Id.* at 30.

We agree with Michaels and Millard’s emphasis on social things, but we respectfully disagree that the “file” is the right abstraction to attach property rights to. The first problem is that while files can be useful ways to refer to data, other groupings of information can be relevant too. Because thinghood is social, how things are identified can change depending on what is useful to talk about — for example, it can be a storm and not many raindrops; a swarm and not many insects; one machine and not several gears. We speak of “the good silverware” rather than identifying thirty-two knives, forks, and spoons, and of “the Frome hoard” rather than 52,503 individual coins.¹¹² Accordingly, just as parcels of land or tangible objects can be joined and severed, it can be useful to think of pieces of data as objects, whose boundaries may vary based on circumstance.¹¹³

A program like Microsoft Word is divided into numerous files on a user’s computer. The files are things, but Word as a whole is also a collective thing, like a swarm or a storm. Neither description is wrong, but one or the other may be more salient. When you “copy” a file on a modern Mac, the underlying data on the solid-state drive is *not* duplicated. Instead, the operating system creates a duplicate *file*, with its own icon and filename, which points to the same *physical location* on the drive. Only if you modify the new version will the computer write the new data to the drive. Until then, the two files, old and new, are simply different names for the same physical encoding of data.¹¹⁴ And some ways of organizing information on computers do not use files at all! Information may be stored in a database in a way that simply does not use the “file” abstraction in the first place; it may consist of numerous records, or tuples, or objects, none of which

112. Relevance to humans also can cut in the other direction, identifying a thing which may not be physically separate from other similar material. For example, few people regularly reference “a partially-submerged mountain” as a particular thing; there isn’t even really a commonly-used term for the entire formation. However, there is a very common word for the part of the mountain that sticks out above the water — an island. Why doesn’t English have a common term for partially-submerged mountains, when it does have a word for islands? The notion of islands — land surrounded by water — is one that is particularly useful for people to be able to use, and the notion of partially-submerged mountains is not.

113. Cf. Margot E. Kaminski & Guy A. Rub, *Copyright’s Framing Problem*, 64 U.C.L.A. L. REV. 1102 (2017) (explaining practical concerns with how judges frame copyrighted works as small or large).

114. Frege would say that they have different *senses* but the same *reference*.

are stored as individual files or in a file that clearly corresponds to a human-meaningful collection of information.

Thus, a “file” as defined by a computer system is not always the relevant thing for property-law purposes. Suppose that a hacker breaks into Kyle Goodwin’s account, downloads a video, reuploads a copy, and then deletes the original. A naïve file-focused account of this process would say that the hacker has wholly destroyed a thing of Goodwin’s: the original file. But from Goodwin’s perspective, the hacker has not destroyed his property, merely interfered with it slightly. He still has access to all of the information he started with, in almost exactly the same form. This sounds more like a minor trespass to chattels than like conversion. The problem is that the “file” as defined by the specific technical affordances of a computer’s operating system is not identical to the data that users care about. Ordinary usage would say that the *data* is sometimes unaffected by changes to the specific *file* that is identified as an abstraction by the computer’s operating system.

One could try to refine this idea by defining property rights in specific physical instances of data, regardless of the interface abstractions used to present them to users. If successful, such an approach would still be an improvement over the *status quo*, which often fails to protect data at all.

But we think a more promising approach is to define the “things” of data in the same kind of way that copyright does with its distinction between a “work” (an informational thing) and a “copy” of a work (a physical object).¹¹⁵ In this definition the work is primary and the copy is secondary. Social consensus on what the work is enables us to mark out specific objects as ones from which the work can potentially be observed. There is thus a coding relationship between work and copy: certain objects encode works in ways that people consider sufficient for observing the work, and these objects are consequently considered to be copies of the work. Different copies have different physical properties but still encode the same work; they can even use drastically different encoding schemes (compare patterns of ink on paper with patterns of electric charge in a computer chip). In philosophical terms, the work is the type and the copies are

115. A physical object is considered a copy of a work when “the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device” from the copy. 17 U.S.C. § 101.

tokens.¹¹⁶ Just as copyright law is ultimately concerned with rights to the work, data property law is ultimately concerned with right to the data.

IV. APPLICATIONS AND REMEDIES

The data property framework solves real-world problems. It protects the important personal and economic interests that individuals and businesses have in data, without creating improvident exclusive rights that would prevent valuable and justified uses. This Part illustrates the utility of a data-property approach with a series of case studies.

A. *Thyroff v. Nationwide: Loss of Access to Data*

Personal property law recognizes two similar torts, conversion and trespass to chattels, that protect against the invasion of an owner's right to use a chattel. These torts can be straightforwardly analogized to invasions of an owner's right to use data.

Conversion applies where a tortfeasor's actions justify a remedy equal to the full value of the chattel.¹¹⁷ Among the behaviors that can constitute conversion is complete destruction of the chattel; “[o]ne who intentionally destroys a chattel or so materially alters its physical condition as to change its identity or character is subject to liability for conversion to another who is in possession of the chattel or entitled to its immediate possession.”¹¹⁸

The 2007 case of *Thyroff v. Nationwide Mutual Insurance Company* is a good

116. See generally, Linda Wetzel, *Types & Tokens*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY, <https://plato.stanford.edu/archives/fall2018/entries/types-tokens/> (Edward N. Zalta, ed., Fall 2018).

117. The Restatement (Second) of Torts provides, “Conversion is an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel.” RESTATEMENT 2D OF TORTS § 222A. (“What Constitutes Conversion”). The section goes to list several factors in determining whether conversion has occurred: “(a) the extent and duration of the actor's exercise of dominion or control; (b) the actor's intent to assert a right in fact inconsistent with the other's right of control; (c) the actor's good faith; (d) the extent and duration of the resulting interference with the other's right of control; (e) the harm done to the chattel; (f) the inconvenience and expense caused to the other.” *Id.*

118. *Id.* at § 226.

illustration of the work that conversion can do for data.¹¹⁹ Nationwide Mutual Insurance leased hardware and software to insurance agent Louis Thyroff.¹²⁰ He also used Nationwide's system for personal emails and to store data on customers. When Nationwide terminated its contract with him, as it was allowed to do, it also repossessed its hardware and cut off access to its system, where his personal emails and customer data were stored.¹²¹ Thyroff sued, and the New York Court of Appeals held that his claim for conversion was cognizable under New York law.¹²² The court acknowledged that it had not previously recognized property rights in data that was not merged in a document, such as rivalrous, intangible property like stock certificates.¹²³ Nonetheless, it concluded, "We cannot conceive of any reason in law or logic why this process of virtual creation should be treated any differently from production by pen on paper or quill on parchment. A document stored on a computer hard drive has the same value as a paper document kept in a file cabinet."¹²⁴

Importantly, Thyroff acknowledged that he did not own the computers on which the data was stored. Nationwide had the right to repossess the physical hardware it leased to Thyroff, and Nationwide owned the "centralized computers" to which his data had been uploaded.¹²⁵ Thus, the case turned entirely on whether Thyroff had a property interest in the data that was distinguishable from the physical computers. As the Court of Appeals stated pithily, "[E]lectronic documents and records stored on a computer can also be converted by simply pressing the delete button."¹²⁶

Thyroff makes eminent sense. The Court of Appeals cogently explained why tangibility is a distraction from the real issues at stake. "[I]t generally is not the physical nature of a document that determines its worth, it is the information memorialized in the document that has intrinsic value."¹²⁷ Its thoroughly

119. *Thyroff v. Nationwide Mutual Ins. Co.*, 864 N.E.2d 1272 (N.Y. 2007). For discussion of *Thyroff*,

120. *Id.* at 284–5.

121. *Id.* at 285.

122. *Id.* at 293.

123. *Id.* at 290.

124. *Id.* at 292.

125. *Id.* at 285.

126. *Id.* at 292.

127. *Id.*

common-law analysis is rooted in the history and policy of the conversion tort.¹²⁸ Several scholars have used *Thyroff* to argue for the broader use of the conversion tort to protect against loss of data.¹²⁹

A data-property framework explains, justifies, and generalizes the result in *Thyroff*. Once data is recognized as a form of property, the applicability of the conversion tort follows naturally.¹³⁰ We can now easily say that Thyroff owned the information instantiated in his digital files on Nationwide's system. Their value was the same as it would have been if printed on paper and stored in a file cabinet.¹³¹ When it comes to protecting Thyroff against their loss, there is no good reason to distinguish the two cases.¹³² Conversion should apply to both.

128. *Id.* at 286–91.

129. Caitlin J. Akins, *Conversion of Digital Property: Protecting Consumers in the Age of Technology*, 23 LOY. CONSUMER L. REV. 215, 235 (2010); Mariel L. Belanger, *Amazon.com's Orwellian Gaffe: The Legal Implications of Sending E-Books Down the Memory Hole*, 41 SETON HALL L. REV. 361 (2011);

130. The value of the broader view is that it brings into play all of the other property rights and causes of action, not just conversion. *Cf.* Amber M. Banks, *Please Don't Stop the Music: Using the Takings Clause to Protect Inmates' Digital Music*, 22 VAND. J. ENT. & TECH. L. 121 (2019) (Takings Clause protection against deletion of data); Spence Howden, *Text Messages Are Property: Why You Don't Own Your Text Messages, but It'd Be a Lot Cooler if You Did*, 76 WASH. & LEE L. REV. 1073 (2019) (conversion and trespass); Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77 (2019) (Takings Clause and criminal investigations).

131. *Cf.* RESTATEMENT 2D OF TORTS § 242 cmt a. (“A document is a chattel and is, therefore, itself the subject of property. As such, it may be the subject of a conversion which makes the actor liable . . . for its value. If the document is of peculiar historic, literary, or artistic value, such value may be obtained under ordinary rules of the law of damages.”).

132. *Compare* United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013) (not a violation of the National Stolen Property Act (NSPA) for the defendant to download files from his employer's servers to a home computer), *with* United States v. United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012) (violation of the NSPA for the defendant to print out files from his employer's servers and take the paper home). This is not a rational distinction. Either both Agrawal and Aleynikov should be convictable, or neither should. Since the purpose of the NSPA was to “assist the States' efforts to foil the ‘roving criminal,’ whose [transportation of stolen objects] across state lines stymied local law enforcement officials,” *Dowling v. United States*, 473 U.S. 207, 220 (1985), the better view is that Agrawal should not have been convicted based on the value of the information in the paper he took. Other statutes, like the Economic Espionage Act, make no distinctions between Agrawals and Aleynikovs based on tangibility. *See* Agrawal, 726 F.3d, at 244–48 (upholding EEA conviction); Aleynikov, 676 F.3d, at 79–82 (overturning EEA conviction).

The situation would be different if Thyroff had kept copies of his files on his personal computer as well as on Nationwide's system. While data property arises out of a person's control over *some* instance of the data, it is not particularly concerned with individual instances or copies, so long as the data remains within the owner's control. If Thyroff has other copies of his data, then Nationwide's actions no longer destroy his ability to use that data. Thyroff has lost a copy, but not what truly matters: the data itself.

Under these circumstances, Nationwide's actions bear a stronger resemblance to trespass to chattels. Under the Restatement, trespass to chattels requires intentionally "(a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another."¹³³ Trespass to chattels has a harm threshold: it is only actionable if "the chattel is impaired as to its condition, quality, or value," or "the possessor is deprived of the use of the chattel for a substantial time."¹³⁴

The translation to data property is again straightforward. Nationwide would be liable for "trespass to data" if the deletion impaired the condition of Thyroff's data or his ability to use it. For example, his back-up copy might contain the same information, but stored in a format that is more difficult to use. Alternatively, it might have taken him a substantial time to recover a backup copy and make it usable (e.g., if he kept backups offsite and offline in a form that takes days to recover). But in the run-of-the-mill case where Thyroff only needs to turn on his computer to start using the data again, Nationwide would face no liability for trespass to chattels.

B. Cloud Storage: Bailments of Data

The best way to understand cloud storage in data-property terms is as a *bailment*.¹³⁵ Cloud storage providers are bailees of their customers' data. In the context of personal property, a "bailee" is "someone who receives personal property from

on other grounds (a jurisdictional hook that has since been removed from the EEA)).

133. *Id.* at § 217.

134. *Id.* at §§ 218, 219. *Cf.* *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003) (applying harm threshold to digital intrusions).

135. See Danielle D'Onfro, *The New Bailments*, 97 WASH. L. REV. 97 (2022). Another virtue of using bailment law is that it helps get other bodies of law right. See, e.g., Michael J. O'Connor, *Digital Bailments*, 22 U. PA. J. CONST. L. 1271 (2020) (Fourth Amendment).

another, and has possession of but not title to the property. A bailee is responsible for keeping the property safe until it is returned to the owner.”¹³⁶ Bailments of data are incredibly common: from Dropbox to Google Docs to Amazon Web Services, millions of people and businesses enter into bailments to store their valuable data.

The fundamental obligations of a bailee are to “exercise ordinary care to protect the subject of the bailment from negligent loss, damage, or destruction”¹³⁷ and to “return the property that is the subject of a bailment to the bailor.”¹³⁸ These duties can be varied by contract, but in the absence of one, property law defines the bailee’s duties. Return of the data is straightforward. The bailee is not obligated to continue hosting the data forever; rather, it must allow the bailor to copy the data onto its own storage.

Of greater interest is the possibility that hosting services will lose their customers’ data. Suppose that a hacker breaks in to Dropbox and deletes users’ data. “Clearly, this is a perfect set-up for an action against the hacker.”¹³⁹ But what about Dropbox’s obligations as a bailee? Unsurprisingly, we already see these services taking steps to limit their liability by contract.

Interestingly, Dropbox already acknowledges some kind of intuitive notion of data property. Its terms of service state, “When you use our Services, you provide us with things like your files, content, messages, contacts, and so on (‘Your Stuff’). Your Stuff is yours. These Terms don’t give us any rights to Your Stuff except for the limited rights that enable us to offer the Services.”¹⁴⁰ The capitalized, and surprisingly informal, term of art *Your Stuff* emphasizes that users’ data *qua* data is something that can be owned and thus could matter for property law.

But Dropbox doesn’t take the notion that files kept in a Dropbox account are “yours” as far as a true bailee would. Later in the agreement, Dropbox emphasizes, in all-capital letters, that it provides its storage services “as is,”¹⁴¹ and

136. BLACK’S LAW DICTIONARY (11th ed. 2019).

137. AM. JUR. 2D, *Bailments* § 77.

138. *Id.* § 129.

139. Robert L. Rabin, *Perspectives on Privacy, Data Security and Tort Law*, 66 DEPAUL L. REV. 313, 329 (2017)

140. Dropbox Terms of Service, <https://www.dropbox.com/terms> (last visited Aug. 18, 2022).

141. “We strive to provide great Services, but there are certain things that we can’t guarantee. TO THE FULLEST EXTENT PERMITTED BY LAW, DROPBOX AND ITS

it further tries to disclaim liability for accidentally deleting users' data.¹⁴² Notably, Dropbox recognizes that it may not be able to disclaim liability for losing its clients' data everywhere, but its terms of service do their best to avoid liability where possible. Other services' terms are similar.¹⁴³ The Amazon Web Services Customer Agreement says that services are provided "as is," disclaiming "all warranties . . . (iii) that the service offerings or third-party content will be uninterrupted, error free or free of harmful components, and (iv) that any content will be secure or not otherwise lost or altered."¹⁴⁴ The agreement goes on to emphasize that "neither we nor any of our affiliates or licensors will be responsible for any compensation, reimbursement, or damages arising in connection with: . . . (d) any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of your content or other data."¹⁴⁵

It is no surprise that data storage services try to avoid liability for losing or

AFFILIATES, SUPPLIERS AND DISTRIBUTORS MAKE NO WARRANTIES, EITHER EXPRESS OR IMPLIED, ABOUT THE SERVICES. THE SERVICES ARE PROVIDED "AS IS." WE ALSO DISCLAIM ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some places don't allow the disclaimers in this paragraph, so they may not apply to you." *Id.*

142. "In countries where exclusions or limitations of liability are allowed, Dropbox, its affiliates, suppliers or distributors won't be liable for: I. Any indirect, special, incidental, punitive, exemplary, or consequential damages, or II. Any loss of use, data, business, or profits, regardless of legal theory. These exclusions or limitations will apply regardless of whether or not Dropbox or any of its affiliates has been warned of the possibility of such damages. If you use the services for any commercial, business, or re-sale purpose, Dropbox, its affiliates, suppliers or distributors will have no liability to you for any loss of profit, loss of business, business interruption, or loss of business opportunity. Dropbox and its affiliates aren't responsible for the conduct, whether online or offline, of any user of the services." *Id.* (printed in all capital letters in original).
143. See also D'Onfro, *supra* note 135, at 142–45 (discussing cloud storage services' contracts).
144. The fuller text disclaims "all warranties, including any implied or express warranties (i) of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, (ii) arising out of any course of dealing or usage of trade, (iii) that the service offerings or third-party content will be uninterrupted, error free or free of harmful components, and (iv) that any content will be secure or not otherwise lost or altered." Amazon Web Services Customer Agreement, <https://aws.amazon.com/agreement/> (last visited Aug. 18, 2022) (printed in all capital letters in original).
145. *Id.* (printed in all capital letters in original).

damaging one's data — indeed physical storage rental service agreements try to do the same thing.¹⁴⁶ Under current law, the fact that self-storage facilities are storing physical property changes the background rules. Physical storage services are unlikely to be able to disclaim liability for intentional destruction of stored property, and some state laws also serve to protect tenants' interests in the content of their storage units.¹⁴⁷ This distinction might be worth maintaining in a world of data property, because what is reasonable for a bailee to do may differ for physical and data property. For example, because people and companies can make many copies of their data, and because computers fail, we might both expect clients to keep additional instances of their data and for storage services to maintain additional backups. So both the defaults of data bailments and the degree to which those defaults can be varied by contract might be different than for bailments of chattels.

Our point is not that bailment law must be identical in every detail for data and chattels. Rather it is that treating data as property makes it easier to get these details right. Recognizing the fundamental similarity between bailments of physical things and bailments of informational things allows legal institutions to evaluate and protect both data owners and data storage providers' interests. A well-calibrated regime of data bailments could allow disclaimers and limitations of liability in some circumstances, but not others, based on considerations like fairness, efficiency, bargaining power, foreseeability, and standard practice.

Notably, bailment law has already played a role in legal cases concerning the loss of electronic data, at least where in cases where a bailee also had or lost the physical computer the data was stored on. *Bridge Tower Dental, P.A. v. Meridian Computer Center, Inc.* held that under the law of bailment, a computer service provider was negligent when it destroyed data on a hard drive.¹⁴⁸ And *DW Data, Inc. v. C. Coakley Relocation Systems, Inc.* awarded replacement costs to a bailor for lost servers and the software they contained under a theory of bailment.¹⁴⁹ Data property law allows the concept of bailment to play a role even when the location

146. See, e.g., Anita Byer and Martin Salcedo, *Rental Agreements Help Self-Storage Operators Limit Liability Exposure*, INSIDE SELF STORAGE, July 8, 2012, <https://www.insideselfstorage.com/insurance/rental-agreements-help-self-storage-operators-limit-liability-exposure>.

147. See *id.*

148. 152 Idaho 569 (2012).

149. 951 F.Supp.2d 1037 (N.D. Ill. 2013).

and state of a particular physical computer is not at issue.

C. *Unauthorized Copying of Data*

Consider now a case involving unauthorized *copying* of data rather than unauthorized *deletion* of data. Suppose that a bookstore keeps a copy of its inventory list on a USB drive, which an employee leaves lying on the store counter. A customer takes the USB drive, copies the inventory list to their own computer, and puts the USB drive back on the counter. The bookstore is entitled to a remedy against the customer, but not because data property creates any new rights. The inventory list is a trade secret, and the customer has misappropriated it by acquiring it through “improper means.”¹⁵⁰ Use of the USB drive is improper under the circumstances — it is “theft . . . or espionage through electronic or other means”¹⁵¹ — because it is a wrongful “using or intermeddling” under the law of personal property.¹⁵²

In other words, this result arises from the combination of two existing bodies of law. Personal property law defines the circumstances under which use of another’s copy of data is wrongful, and trade secret law defines the remedies available to the owner for the wrongful acquisition and use of that data. In our view, these are the right lenses through which to view this issue. Both bodies of law attempt to strike a balance between owners’ interests in data and its embodiments, and other people’s interests in being able to use and share information freely.

Our data property framework does not expand liability beyond its current scope. If this modesty seems curious, consider a similar hypothetical which does not trigger intuitions about the bookstore’s business interests. Suppose that the bookstore has downloaded copies of several public-domain novels from Project Gutenberg onto the USB drive.¹⁵⁴ The customer copies the novels onto their own computer, but does not alter the copies on the bookstore’s USB drive. Here, there is no trade-secret claim, because these novels are “readily ascertainable by proper

150. Uniform Trade Secrets Act § 1(2)(i) [hereinafter UTSA].

151. *Id.* § 1(I).

152. RESTATEMENT (SECOND) OF TORTS § 217(b). Note that one can commit trespass to chattels without incurring liability. *See id.* cmt. A. The interference is wrongful, even if it is not independently actionable.

154. Project Gutenberg, <https://www.gutenberg.org/> (last visited Aug. 18, 2022).

means” by anyone else who downloads them from Project Gutenberg.¹⁵⁵ Similarly, the customer used the bookstore’s USB drive without consent, but a brief use that doesn’t damage the drive or interfere with the owner’s own use of it does not by itself create trespass-to-chattels liability. So there is no liability under existing law, nor should there be. From a data-property perspective, the bookstore and its employees are still free to enjoy the books — its “right to use” the digital novels may have been temporarily interfered with while the customer was using the USB key, but that interference was brief and *de minimis*.¹⁵⁶

A similar analysis applies where the defendant copies the data over the Internet, rather than in person. Here, the laws that define whether the defendant’s access is wrongful include trespass to chattels (with the same threshold that liability lies only when “the chattel is impaired as to its condition, quality, or value”¹⁵⁹ or “the possessor is deprived of the use of the chattel for a substantial time”¹⁶⁰) and also computer-misuse laws such as the Computer Fraud and Abuse Act.¹⁶¹ So while it is wrongful under these access-control laws to hack into a computer to gain access to another’s data and copy it, it is not wrongful under them to copy information that one has been given access to.¹⁶² If the bookstore has a website with a page for each book in its inventory, a competitor is free to download those pages and reconstruct the complete list of books the bookstore carries. Recognizing the bookstore’s data property in its inventory list does not require changing this result. By putting up a website that embodies the inventory list, the bookstore has given its consent for others to copy that data.

We acknowledge that in some cases, a defendant might gain tremendous value from copying an owner’s data without permission, and that in such cases, some might strongly advocate for some law to prevent the defendant from gaining a significant benefit through a wrongful act, even if the underlying data was not protected as a trade secret or through any other intellectual property law. However, a new body of data property need not and should not be implicated in addressing this type of wrong, when the law of unjust enrichment already covers

155. UTSA § 1(4)(i).

156. RESTATEMENT (SECOND) OF TORTS § 218(c).

159. *Id.* § 218(b).

160. *Id.* § 218(c).

161. 18 U.S.C. § 1030.

162. *Van Buren v. United States*, 141 S. Ct. 1648 (2021); *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019).

this concern. The law of unjust enrichment would likely rarely apply, because it typically links one party's gain with another's loss.¹⁶³ However, where conscious wrongdoing is involved, the Restatement of Restitution and Unjust Enrichment contemplates that disgorgement could be an appropriate remedy when an unjust gain is greater than the harm to a claimant.¹⁶⁴ Care must be taken in defining which means of copying data under the owner's control are wrongful as an initial matter, and care must be taken in measuring how much of the defendant's gain is actually attributable to the wrongful copying. But framing this problem as a *property* problem brings the right analytical tools to bear: these are precisely the kinds of questions that the law of restitution already grapples with.

The most difficult case is one in which someone wrongfully copies another's information without permission and then shares it with an innocent third party. As with the previous examples, data property law does not affect the outcome. The law of restitution again indicates that the third party should be able to use the data unless she was conscious her acquisition of the data is wrongful.

In the context of data acquisition, limiting the scope of unjust enrichment law to conscious wrongdoing is necessary to prevent the notion of "data property" from metastasizing into an eternal, unlimited intellectual property right. Public domain materials are often available on the Internet, or in libraries or personal collections, without any affirmative indication of where they came from. That they *might* have been acquired, proximately or ultimately, through a wrongful act should not limit how those materials can be used, nor should potential users have any obligation to investigate the origins of otherwise public-domain materials. Creating an obligation to inquire about the origins of ostensibly public-domain or factual materials will create an undesirable chilling effect on the

163. For example, the Restatement (Third) of Restitution and Unjust Enrichment states plainly, "A person who is unjustly enriched *at the expense of another* is subject to liability in restitution." RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (emphasis added).

164. The Restatement provides, "Restitution requires full disgorgement of profit by a conscious wrongdoer, . . . because any lesser liability would provide an inadequate incentive to lawful behavior. If A anticipates (accurately) that unauthorized interference with B's entitlement may yield profits exceeding any damages B could prove, A has a dangerous incentive to take without asking." RESTATEMENT 3D OF RESTITUTION AND UNJUST ENRICHMENT § 3 cmt. c. For this reason, the Restatement concludes that, "A person is not permitted to profit by his own wrong." *Id.* at § 3.

use of this material. Individuals and businesses would be afraid to use public domain or otherwise unprotectable content, out of concern that it might have been wrongfully acquired and that a court might conclude that they “should” have known this. Intermediary parties, such as publishers or distributors, might not want to take risks on publishing or distributing such material for similar reasons. Second, any standard short of “conscious wrongdoing” would circumvent the policy judgments about scope already made in other intellectual property regimes and legal regulations covering use of personal data.

D. Sharing Data in Violation of an Agreement

Another form of wrongful copying involves sharing data in violation of an agreement. Suppose a farmer makes a contract with an organization studying climate change and weather patterns to provide statistical information about rainfall on his farm over the year. As part of the contract, the organization agrees not to share the information with others. Nonetheless, it does share the rainfall data with a prospective land purchaser.

Trade secret law might cover this situation. If the farmer’s information was covered by trade secret law, the data-gathering organization would have had an obligation not to pass it on.¹⁶⁵ Moreover, depending on what the land purchaser knew or had reason to know about the status of the information he was receiving, he might or might not be liable for misappropriating a trade secret.¹⁶⁶

But even without trade secret protection, the data-gathering organization would be liable for breach of contract with the farmer, and depending on the land buyer’s state of mind and behavior, the buyer might be liable for tortious interference with a contractual relationship.¹⁶⁷ Once again, the availability of

165. Uniform Trade Secrets Act § 1(2)(ii)(B)(II) (defining misappropriation of a trade secret to include “disclosure or use of a trade secret of another without express or implied consent by a person who . . . at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was . . . acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.”)

166. *Id.* at § 1(2)(i) (defining misappropriation of a trade secret to include “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means”); *id.* at § 1 (defining improper means as including “breach or inducement of a breach of a duty to maintain secrecy”)

167. *See Cocoli v. Town of Scituate Town Council*, 184 A.3d 1113, 1120 (R.I. 2018) (“In order to establish a claim for tortious interference with a contractual relationship, plaintiffs must

either of these actions does not depend on recognizing property rights in data. Recognizing data property rights is useful because it clarifies the questions at issue, and may help calculate damages or the value of the contract. But recognizing data-property rights does not extend liability to any new parties in this situation.

E. Medical Information about Patients

Suppose a patient is being treated by a doctor who stores his patient files with MedCloud.¹⁶⁸ Due to misconfigurations and failure to effectively use encryption, MedCloud suffers a data breach and the patient's health information is obtained by hackers. What does this state of affairs look like in data property terms?

The third-party hackers committed property torts against MedCloud's personal property and against the doctor's data property. As between the doctor and MedCloud, the doctor has also suffered a harm to her right to exclude others from her data property in her patient files because her bailee allowed third parties to obtain her data property without her authorization. Her contract with MedCloud may or may not absolve it from liability here; this is, as we noted above, an issue of bailment law.

The patient, however, is *not in the property picture*. The fact that the health data concerns him gives him no data property rights in it. It is data about him, but it he does not have control over any instances of it. The doctor and MedCloud do, so when the hackers interact with those instances, it implicates the doctor and

establish the following four elements: (1) [T]he existence of a contract; (2) the alleged wrongdoer's knowledge of the contract; (3) his [or her] intentional interference; and (4) damages resulting therefrom."); *Downs v. Homax Oil Sales, Inc.*, 421 P.3d 518, 524 (Wyo. 2018) ("The specific elements of a claim for tortious interference with contract or prospective contractual relation are: (1) The existence of a valid contractual relationship or business expectancy; (2) knowledge of the relationship or expectancy on the part of the interferer; (3) intentional and improper interference inducing or causing a breach or termination of the relationship or expectancy; and (4) resultant damage to the party whose relationship or expectancy has been disrupted."); RESTATEMENT 3D OF TORTS § 16 ("A defendant is subject to liability for interference with contract if: (a) a valid contract existed between the plaintiff and a third party; (b) the defendant engaged in wrongful conduct . . . ; (c) the defendant intended to cause a breach of the plaintiff's contract or disruption of its performance; and (d) the defendant's wrongful conduct caused a breach of the contract or disruption of performance.").

168. See MedCloud, <https://medcloud.link/elements/about> (last visited Aug. 18, 2022).

MedCloud's property rights, not the patient's. Data property law extends personal property law by giving the *doctor* the right to sue the hackers, but it does not extend to giving the *patient* similar rights.

This is not to say that the patient has no rights here. The doctor may have violated her duties to the patient by improperly storing his files on MedCloud. The doctor and MedCloud may have violated the Health Insurance Portability and Accountability Act ("HIPAA");¹⁶⁹ they may have violated state statutory privacy law like the California CPA;¹⁷⁰ MedCloud may have engaged in an unfair and deceptive trade practice by storing information without proper security.¹⁷¹ Some of these bodies of law may give the patient a right of action against the doctor or MedCloud. But these are *privacy-specific* rights of action; they pertain to the handling and mishandling of information about people in specific ways. As explained in Section III.D.1, data property law functions in parallel to and consistently with these privacy rights and regulations.

F. Data Taken from Patients' Bodies: Explaining Moore

The case of *Moore v. Regents of the University of California*,¹⁷² concerning property in information derived from patients' bodies, is a staple of property casebooks and scholarship. It is also frequently misunderstood. Distinguishing data property from tangible property and intellectual property helps cut through some of the confusion.

In brief, John Moore underwent treatment for hairy-cell leukemia at the UCLA Medical Center. After removing his spleen, his doctors had him return for follow-up visits at which they took numerous tissue samples. They used portions of his spleen to isolate and reproduce some of his T-cell lymphocytes, establishing a "cell line" of cells genetically derived from Moore's lymphocytes. They applied for and received a patent on the cell line, and licensed it for commercial development.¹⁷³ The California Supreme Court held that on these facts, Moore

169. Pub. L. 104-191, Aug. 21, 1996, 110 Stat. 1936.

170. Cal. Civ. Code §§ 1798.100-.199.

171. See *Federal Trade Comm. v. Wyndham Worldwide Corp.* 799 F.3d 236, 244-47 (3d. Cir. 2015) (concluding that a company's failure to maintain appropriate data security could constitute an unfair trade practice under 15 U.S.C. § 45).

172. 51 Cal. 3d 120 (1990).

173. *Id.* at 125-128.

failed to state a cause of action for conversion.¹⁷⁴ The court did, however, allow him to proceed on a claim of breach of fiduciary duty against the doctor who failed to disclose his intended research and his financial interests in it before the splenectomy.¹⁷⁵

Although *Moore* remains deeply controversial, a data-property perspective shows that its holdings were sound. Moore voluntarily relinquished any *personal property* interests in the tangible cells extracted from his body when he allowed his doctors to take samples.¹⁷⁶ He lacked any personal property interests in the T-cell lymphocytes developed from his own T-cell lymphocytes because they were new cells that had never been part of his body, and his lack of property interests in the extracted cells meant he could claim no rights over the developed ones under the rule of increase.

Moore also lacked any *intellectual property* interests because he did not qualify as an “author” of any information in his cells, as an “inventor” of the cell line, and so on.¹⁷⁷ To be sure, these rules embody contestable normative choices about what kind of effort, investment, creativity, personality, etc. qualify for intellectual property rights over pure information.¹⁷⁸ It is possible to imagine a world in which people enjoy intellectual property rights to prevent identified unauthorized uses of genetic information derived from their cells. But this is not our world, and to be clear, these would be *intellectual property* rights. They would derive from the fact that a person has specific genetic information embedded in their body, and would vest that person with a right over that information *as such*, regardless of how it was extracted.

Data property clarifies why the fiduciary-duty claim was the right vehicle to vindicate Moore’s interests. Moore’s doctors used their physician-patient relationship with him to obtain possession of instantiations of the information in his cells. From there, they made more instantiations and carried out various

174. *Id.* at 147.

175. 51 Cal.3d at 129-133.

176. In fact, because of the special treatment of body parts under property law, personal property rights in cells are more limited than rights to other tangible things. *See, e.g., Newman v. Sathyavaglswaran*, 287 F.3d 786 (9th Cir. 2002).

177. We could explain at tedious length why he had no trademark rights, right of publicity rights, boat-hull design rights, plant variety protection rights, and so on, but the pattern should be clear.

178. *See* JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS (1996).

further derivations. In data-property terms, performed medical procedures on him *to become possessor-owners of data property*, which they then used as a substantial input into a research process that produced valuable personal property (the cells), data property (the cell line), and intellectual property (the patent).

So described, it is clear that Moore's claim is properly grounded in the initial access to the information in his body. Moore had possession of the information in his cells, as every person does. Because data property is non-exclusive, other people can also have possession of that information (e.g., one's relatives, with whom one naturally shares some genetic information by biological inheritance); use of instances possessed by others does Moore no data-property harm. It is the extraction of the information *from an instance in his possession* without his permission that data-property law forbids. A claim for breach of fiduciary duty and lack of informed consent exactly captures the nature of the wrong.

V. CONCLUSION

We come to clarify and to codify, not to declare a digital revolution. If you believe in personal property, you should believe in data property. Even “the most resolute communist societies,” use property to organize the use of resources to at least some degree.¹⁷⁹ They do so because property rights solve resource coordination problems by creating workable systems for how people use tangible objects.¹⁸⁰ With only limited exceptions, the overwhelming majority of people across cultures maintain both a practice of keeping personal property themselves and a belief that government and society should recognize and protect one's personal property.¹⁸¹

The specific things that matter to people have changed, but not the age-old human values that explain why those things matter. Family photos live in digital

179. Merrill, *supra* note 28, at 2062.

180. See Thomas W. Merrill & Henry E. Smith, *The Morality of Property*, 48 WM. & MARY L. REV. 1849, 1850 (2007) (“Property is a device for coordinating both personal and impersonal interactions over things.”); Thomas W. Merrill, *The Property Strategy*, 160 U. PA. L. REV. 2061, 2062 (2012). See generally Cohen, *supra* note 19.

181. E.g., Abraham Bell & Gideon Parchamowsky, *Property Lost in Translation*, 80 U. CHI. L. REV. 515, 520 (2013) (“Originally, kibbutzim absolutely prohibited private property However, over time, socialism declined in popularity in Israel Nowadays, only a few kibbutzim retain a collective property system; all the rest — several hundred of them — have succumbed to the pressure and opted for some version of private property.”).

albums on computers, not just in framed albums on the mantel. The books on our shelves, the files in our cabinets, and the letters in our shoeboxes have all become virtual. Property law is a poor shadow of what it used to be if it protects only the physical shelves, cabinets, and shoeboxes — and not the ebooks, spreadsheets, and emails that truly matters. Whether you believe that property rights allow people to plan for the future, promote the efficient use of things, support a democratic society, or protect personhood, in our society today, digital things do all of these just as much and just as well as physical things do. They deserve no less respect from the law.¹⁸²

We introduce here no new or radical ethic. This Article calls for only mild changes in the law. It proposes the extension of existing torts to protect against the wrongful loss of data. These changes are badly needed, but they are small. Data property does not open the gate to the wholesale propertization of personal information; it does not create a new and sprawling form of intellectual property. Our point in showing how closely data property fits within the existing personal-property framework is precisely to show that these dangerous and far-reaching changes are unnecessary. The sky will not fall if the law recognizes data property.

The lay user who speaks of “their” data is not wrong; it is the theoretical constructs of property law that need to change. We have explained how data is a thing, how that thing can be possessed and controlled, and how ownership of that thing can be protected. In short, data is property.

182. As Margaret Radin poetically argued, “If an object you now control is bound up in your future plans or in your anticipation of your future self, and it is partly these plans for your own continuity that make you a person, then your personhood depends on the realization of these expectations.” Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 968 (1982).