PERSONAL DATA AS PROPERTY

Steven H. Hazel†

TABLE OF CONTENTS

† J.D., University of Chicago Law School. Thanks to Professors Nicholas Stephanopoulos and William H. J. Hubbard as well as to participants in the University of Chicago Law School's Canonical Ideas in Legal Thought seminar for comments on earlier drafts of this work. All errors are mine.

ABSTRACT

Today, a growing chorus of experts, journalists, and policymakers calls for the creation of property rights in personal data. In theory, property rights emerge when the gains from propertization outweigh the costs of securing those rights. This formula, originally identified by Harold Demsetz, explains the development of property rights in land, intellectual property, and many other assets.

Applying Demsetz's theory, this Article asks whether the time has come to extend property rights in personal data. The answer is yes.

The first half of Demsetz's formula estimates the gains from extending property rights. Under the contract-law-based status quo, the market for personal data suffers from high information and enforcement costs along with inadequate incentives to supply and safeguard data. Propertization promises to mitigate—though not completely resolve—those challenges.

The second half of Demsetz's formula trains on the cost of securing property rights. For property rights to be secure in practice—not just desirable in theory—institutional investments are necessary. The

conventional wisdom holds that only state-run institutions, such as courts and regulators, can protect property. But rather than rely solely on regulators and courts, policymakers should deputize private adjuncts to define and enforce property rights. This approach enlists efficient managers of information—data processing firms—in securing property. Compared with a propertization regime that relies on state-run institutions, mobilizing private adjuncts promises to substantially lower the cost of securing property rights.

Because the gains from propertization are larger, and the costs smaller, than previously thought, both prongs of Demsetz's formula favor the creation of property rights in personal data.

INTRODUCTION

A growing chorus of experts, policymakers, and consumer advocates call for the creation of property rights in personal data. Most important, the European Union's General Data Protection Regulation (GDPR), the leading global privacy regime, encourages consumers to treat data as property.[1] New or proposed legislation in Brazil, California, and India follows suit.[2] Even leading technology companies invite their customers to understand data as property. Microsoft, for instance, promises to "put[ ] customers in control of their own data."[3]

So far, American law has generally refused to recognize property rights in data.[4] But property rights are not static. As Harold Demsetz observed, "property rights develop to internalize externalities when the gains of internalization become larger than the cost of internalization."[5]

1. *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 Council Directive 95/46/EC, 2016 O.J. †L 119) [hereinafter GDPR].

2. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (Deering, LEXIS through 2020 Reg. Sess.); *see generally* Joseph Jerome, *California Privacy Law Shows Data Protection Is on the March*, 33 ANTITRUST 96 (2018) (discussing the California Consumer Privacy Act and similar legislation in Brazil and India).

3. *See* Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

4. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 695 (7th Cir. 2015) (finding "no authority" that "federal law recognizes such a property right" in personal data).

5. *See* Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 350 (1967) ("[T]he emergence of new private or state-owned property rights will be in response to changes in technology and relative prices.").

This simple formula predicts when property rights will emerge.[6] Consider land, the most familiar form of property. Early in human history, land was plentiful, so there was little to gain from developing property rights.[7] But as the population expanded, land grew scarce.[8] By the Middle Ages, the gains of internalization began to outweigh the costs of internalization, and property rights emerged.[9] A similar progression explains the development of property rights in intellectual property,[10] air,[11] and land in the American West.[12] In each case, an increase in the underlying value of an asset, coupled with improvements in the institutions available to secure that asset, triggered the emergence of property rights.[13]

This paper asks whether the time has come to grant property rights in personal data. The answer is not obvious. Indeed, academics have debated the merits of propertization for the past two decades.[14] Even now, propertization continues to spark scholarly discussion.[15] By applying

6. *See* DOUGLASS C. NORTH & ROBERT PAUL THOMAS, THE RISE OF THE WESTERN WORLD: A NEW ECONOMIC HISTORY 4–5 (1973). In a separate work, North described the absence of property rights as one of "the most important source[s] of both historical stagnation and contemporary underdevelopment in the Third World." *See* DOUGLAS C. NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 54 (1990).

7. *See* NORTH & THOMAS, *supra* note 6, at 19.

8. *See id.*

9. *See id*.

10. The increasing value of inventions, in combination with new technologies to protect ideas, has corresponded with the creation of intellectual property rights. Writing in 1973, North and Thomas observed that "[r]ight to the present day, technical problems have made it similarly difficult, and therefore costly, to develop and enforce property rights in ideas, inventions, and innovations . . . ." *Id.* at 5.

11. Soon after the Wright brothers invented the airplane, property rights in airspace developed. *See* TERRY L. ANDERSON & FRED S. MCCHESNEY, PROPERTY RIGHTS: COOPERATION, CONFLICT AND LAW 38 (2003).

12. *See id*. (discussing how the invention of barbed wire led to the installation of property rights in the American West).

13. Either the government or private parties must invest in defining and enforcing those rights. *See* NORTH & THOMAS, *supra* note 6, at 3.

14. *See generally e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data,* 117 HARV. L. REV. 2055 (2004) (adding to the debate by seeking to develop a model for properitization of personal data that will fully safeguard information privacy); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000) (arguing that achieving consensus on the rationale for information privacy protection may be unnecessary if both economic and noneconomic considerations favor greater protection for personal data); Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2003) (arguing that in order to protect privacy, individuals must secure control their personal information by becoming its real owners). Part II.B surveys the main objections to propertization raised by this scholarship.

15. *See generally e.g.*, Vlad A. Hertza, *Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?*, 93 N.Y.U.L. REV. 1707 (2018) (proposing solutions inspired by GDPR to resolve issues in consumer credit reporting); Jeffrey Ritter & Anna Mayer, *Regulating Data As Property: A*

Demsetz's formula, this paper contributes two insights that upend that debate.

First, Demsetz teaches that understanding "the gains from internalization" requires a comparison between the proposed property regime and the status quo.[16] Today, data subjects and data processing firms routinely exchange personal data.[17] For the most part, contract law governs those trades.[18] But the status quo suffers from pervasive market failures, including excessive information and enforcement costs along with inadequate incentives to supply and safeguard personal data.[19] Classifying personal data as property promises to alleviate, though not completely resolve, these shortcomings.[20] Ultimately, comparing the contract-based status quo with a hypothetical property regime reveals that the gains from propertization—the first half of Demsetz's formula—may be significant.

Second, Demsetz recognized that the appeal of propertization turns not only on the gains from extending property rights, but also on the cost of securing those rights.[21] As scholars observe, "property cannot exist without some institutional structure that stands ready to enforce it."[22] At first glance, protecting property rights in personal data promises to be especially difficult. Thanks to personal data's unique attributes—the high volume in which it is produced and the ease at which it is copied and

New Construct for Moving Forward, 16 DUKE L. & TECH. REV. 220 (2018) (proposing that regulation of digital information assets, and clear concepts of ownership, can be built on existing legal constructs that have enabled electronic commercial practices).

16. *See* Demsetz, *supra* note 6, at 350. For an early look at the status quo, *see* Schwartz, *supra* note 15, at 2117 (asking how propertization would affect four different technologies). Schwartz described the status quo in 2004, and focused on some technologies that have not stood the test of time, such as compensated telemarketing. *See id.* at 2122–25.

17. These terms will be used throughout the Article. According to the definitions in GDPR, a *data subject* is "an identifiable natural person;" a *data processor* is "a natural or legal person, public authority, agency or other body which processes personal data;" and personal data is "any information relating to an identified or identifiable natural person." GDPR, *supra* note 1, art. 4(1); (8).

18. *See* Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U.L. REV. 662, 663 (2019).

19. *See infra* Part I.B.3 (discussing these failures in detail).

20. *See infra* Part II.A (arguing that extending property rights in personal data would improve the status quo).

21. Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 733 (1998). Douglass North defines institutions as "rules of the game" and "humanly devised constraints that" shape human interaction. Douglass C. North, *Institutions*, 5 J. ECON. PERSPECTIVES 97, 97, 98 (1991).

22. Merrill, *supra* note 23, at 733 ("Given that property is a norm, there is also a consensus that property cannot exist without some institutional structure that stands ready to enforce it. The usual assumption is that this institution is the state.").

transferred—extending property rights in that data may require costly institutional investments.[23]

This paper outlines a strategy for securing property rights in personal data.[24] The conventional wisdom assumes that only state-run institutions, such as courts and regulators, protect property.[25] But the state need not hold a monopoly on securing property rights. Rather than rely exclusively on regulators and courts, policymakers should deputize private adjuncts to define and enforce property rights.[26] Protecting property rights depends on managing information, such as storing ownership records and monitoring interlopers. That is what data processing firms do best. At the same time, while government enforcers struggle to overcome personal data's unique attributes, private adjuncts harness those features to ease enforcement. Compared with the conventional, state-dominated approach, private adjuncts promise to secure property rights in personal data cheaply, quickly, and effectively.

Because the gains from propertization are larger, and the costs smaller, than previously thought, both prongs of Demsetz's formula favor the creation of property rights in personal data.

This Article proceeds as follows. Together, Parts I and II examine the first half of Demsetz's formula: the gains from granting property rights in personal data. Part I documents the market failures that currently plague the personal data economy. Next, Part II contends that a hypothetical property regime would improve upon—although not perfect—the status quo. Investing in property rights promises to correct several distortions in the market for personal data, yielding benefits for both data subjects and data processors.

Parts III and IV turn to the second half of Demsetz's formula: the institutional investments necessary to secure property rights. Consistent with the finding that property rights improve the status quo, Part III introduces the European Union's (E.U.) General Data Protection Regulation (GDPR) a regulation that can be understood as granting property rights.

23. *See infra* Part I.A (identifying the features that distinguish personal data from traditional forms of property).

24. *See infra* Parts IV.A & IV.B (proposing five institutions to define and enforce property rights in personal data).

25. *See infra* Part IV (discussing two such studies).

26. Economists increasingly recognize the importance of informal institutions. *See, e.g.*, Claudia R. Williamson & Carrie B. Kerekes, *Securing Private Property: Formal Versus Informal Institutions*, 54 J.L. & ECON. 537, 564 (2011) (observing that "informal institutions are the underlying channels that establish secure, well-defined property rights").

Drawing on examples from GDPR, Part IV argues that private adjuncts promise to secure property rights in personal data cheaply, quickly, and efficiently. To illustrate the virtues of this approach, Part IV demonstrates how GDPR enlists private adjuncts to: (1) identify property owners, (2) account for complementarities, (3) resolve disputes, and (4) enforce rights. Thanks to private adjuncts, the case for extending property rights in personal data is stronger than previously thought.

I. THE CONTRACT-BASED STATUS QUO

In 2005, a federal court declared that "[t]here is likewise no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large."[27] Even then, that conclusion was probably wrong.[28] Today, it certainly is. Every day, consumers exchange enormous volumes of personal data,[29] contributing hundreds of billions of dollars to the global economy.[30]

To evaluate the gains from extending property rights—the first half of Demsetz's formula—it is necessary to understand how personal data markets operate. This Part maps that landscape. First, it identifies two attributes that differentiate personal data from other forms of property: the aggregation imperative and the ease of onward transfer. These attributes go a long way towards explaining existing patterns of data exchange. Next, this Part introduces common transactions that transfer personal data: corporate acquisitions, data broker purchases, and consumer contracts. For the most part, contract law governs these transactions. Finally, this Part pinpoints the market failures that plague this contracts-based status quo. Personal data markets suffer from high information and enforcement costs, distorting consumers' incentives to supply accurate information and firms' incentives to safeguard that information. Part II will examine the extent to which extending property rights promises to address these shortcomings.

A. What Makes Personal Data Different?

In theory, personal data is difficult to define. Indeed, the leading paper identifies three definitions, only to conclude that none are wholly

27. In re Jet Blue Airway's Corp. Privacy Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005).

28. *See, e.g.*, Schwartz, *supra* note 14, at 2094 (noting that "personal data trade" was "already [a] well-established phenomenon" in 2005).

29. *See* ERIC A. POSNER & E. GLEN WEYL, *Radical Markets: Uprooting Capitalism and Democracy for a Just Society* 220 (2018).

30. JAMES MANYIKA ET AL., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 8 (McKinsey & Co. 2011), http://perma.cc/EML6-2ZGR.

satisfying.[31] In practice, however, statutes articulate definitions that succeed in differentiating personal data from other kinds of data.[32] Consistent with the GDPR, this Article defines personal data as any "information relating to an identified or identifiable natural person."[33] Two attributes distinguish personal data from traditional forms of property: the aggregation imperative and the ease of onward transfer. Any legal regime that regulates personal data must account for these features.

1. The Aggregation Imperative

The volume of personal data sets it apart from other assets—even from other forms of intellectual property.[34] According to one estimate, today's society "create[s] as much information in two days as we did from the dawn of man through 2003."[35] Eric Schmidt, the former Chairman of Google, observes that much of this increase comes from "user-generated content"—personal data in the form of pictures, instant messages, and social media posts.[36] Even the Supreme Court has recognized that the enormous amount of personal data distinguishes it from other assets. In *Riley v. California*,[37] the Court emphasized that "[t]he current top-selling smart phone . . . [can hold] millions of pages of text, thousands of pictures, or hundreds of videos."[38] No other asset—whether land, real

31. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1835 (2011) (observing that "[a]ll current legal models for this concept are flawed").

32. *See* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* 48 B.C. L. REV. 609, 632 (2007) (differing personal data from bank account information).

33. GDPR, *supra* note 1, art. 4(1) (noting that "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person").

34. For instance, the U.S. Patent and Trademark Office grants several hundred thousand patent applications in the typical year, a number dwarfed by the volume of personal data that may be present on a single cell phone. *See U.S. Patent Activity, CY 1790 to Present*, P.T.O (June 1, 2018, 3:05 PM), http://perma.cc/5GQZ-9P4W (listing 298,000 utility patents granted in 2015).

35. *See* MG Siegler, *Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up to 2003*, TECH CRUNCH (Aug. 4, 2010), http://perma.cc/WW4R-HNVX.

36. *See id*.

37. 573 U.S. 373 (2014).

38. *Id*. at 394.

property, or even intellectual property—is collected in the same quantity as personal information.[39]

At the same time, personal information usually has economic value only when combined.[40] Large datasets enable predictive algorithms, train artificial intelligence, and contribute to other big data applications.[41] As Amazon Data Scientist Andreas Weigend explains, "[i]n many cases, the true meaning of the data we create emerges only when we're comparing our data to the data created by others."[42] In economic terms, the marginal value of adding each additional data point is non-linear.[43] Thus, 100 pieces of data may be more than 100 times more valuable than one piece of data.[44] As Weigend observes, "[s]ubtract one person's data and the [data] refineries can still arrive at the same conclusions from everything that's left."[45] Personal information is more useful both when processors aggregate the same data point about many people (for example, the political affiliation of every Georgia voter) and when processors combine many types of information about one person (for example, every purchase made by a particular consumer in the last year).[46] Together, the volume of personal data and the fact that its economic value depends on context teach the same lesson. To extract the full value of information, participants in the data economy must aggregate it into large datasets.

2. The Problem of Onward Transfer

Hal Varian, Google's chief economist, observes that "[i]nformation is costly to *produce* but cheap to *reproduce*."[47] Put in economic terms, the, "production of an information good involves *high fixed costs* but *low*

39. *See* Nicole Martin, *How Much Data is Collected Every Minute of the Day*, FORBES (Aug. 7, 2019, 3:34 PM), https://www.forbes.com/sites/nicolemartin1/2019/08/07/how-much-data-is-collected-every-minute-of-the-day/#40e6326f3d66.

40. *See* Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/.

41. *See* POSNER & WEYL, *supra* note 29, at 224–25 (discussing the importance of large datasets, and pointing out that "[t]he [marginal] value of data as a function of the number of observations in a standard statistical estimation problem . . . declines rapidly"). *See also* Part I.C.3 (discussing problems in the market for high-quality data).

42. ANDREAS WEIGEND, DATA FOR THE PEOPLE: HOW TO MAKE OUR POST-PRIVACY ECONOMY WORK FOR YOU 20 (2017).

43. *See id.*

44. *See id.*

45. *Id.*

46. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1881 (2013).

47. CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 3 (1999).

marginal costs."[48] For anyone who has used their computer's copy and paste function, this is not difficult to grasp. The upshot is that it is easy to share information with others, but difficult to restrict the spread of that information.[49] Some commentators call this the "onward transfer" problem.[50] Once a data subject has given up her information, it may be transferred to third parties.[51] But, since information is non-rivalrous, multiple people can use information at the same time without being aware of one another.[52] That makes enforcement a tall order. As Daniel Solove observes, "[i]t is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses . . . ."[53] The existence of the data broker industry, which exists to copy and transfer data without consumers' knowledge, exemplifies this problem.[54]

Ultimately, any legal regime that regulates personal data must account for the aggregation imperative and the ease of onward transfer. The next Section demonstrates that these attributes play an outsized role in shaping existing patterns of exchange.

B. Personal Data Markets

Two decades ago, information researcher Kenneth Laudon proclaimed that, "there is already a lively marketplace in the United States for personal information."[55] Today, that marketplace has grown to affect almost every consumer and organization. To provide a snapshot of the status quo, this Section examines three types of exchange, each at a different scale: (1) corporate transactions, (2) the data broker industry, and (3) consumer contracts. The aggregation imperative and the ease of onward transfer shape each form of exchange.

1. Corporate Transactions

Mergers and acquisitions showcase both attributes of personal data: the aggregation imperative and the ease of onward transfer. First, the need to aggregate personal data motivates many corporate transactions. As it

48. *Id.*

49. *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 324 (2013).

50. *See id.*

51. *See id.*

52. *See id.* at 338.

53. Solove, *supra* note 46, at 1881.

54. For a detailed discussion of the data broker industry, *see infra* Part I.B.2.

55. Kenneth Laudon, *Markets and Privacy*, *in* COMPUTERIZATION AND CONTROVERSY: VALUE CONFLICTS AND SOCIAL CHOICES 705 (Robert King ed., 1996).

stands, firms "spend considerable money and effort to acquire and analyse personal data and to maintain a data-related competitive advantage."[56] This pattern is most obvious in the technology industry, where "[d]ata has become the most important strategic asset."[57] For example, Facebook's $1 billion purchase of Instagram relied on a calculation that "paid $30 for each of the 33 million Instagram users."[58]

But corporate transactions that aim to aggregate data are not limited to technology companies. Take the pending merger between CVS, a retail pharmacy chain, and AETNA, a health insurer.[59] Both companies emphasized that the ability to aggregate personal data inspired the merger.[60] As CVS's CEO explained, "[b]y integrating data . . . we will create targeted interactions with patients to promote healthy behaviors and drive adherence. . . ."[61] That companies engage in multi-billion dollar mergers to consolidate personal data testifies to the importance of aggregation to unlocking the full value of that data.

Second, corporate transactions also illustrate the problems posed by onward transfer. Too often, mergers, acquisitions, and even bankruptcies take advantage of the ease of transferring data to escape privacy commitments enshrined in consumer contracts. Consider Radio Shack's bankruptcy. Many analysts deemed Radio Shack's customer lists and other personal data its most valuable asset.[62] So it is no surprise that Radio Shack attempted to sell its customer data to satisfy creditors. The problem, however, was that creditors would not necessarily be bound by the privacy promises that Radio Shack made to its customers.[63] In a similar vein, after Barnes & Noble bought the personal information of Borders's customers, it "garnered intense FTC scrutiny due to past promises by

56. ALLEN P. GRUNES & MAURICE E. STUCKE, BIG DATA AND COMPETITION POLICY 8 (2016).

57. *See* Pauline Glickman & Nicolas Glady, *What's the Value of Your Data?*, TECH CRUNCH (Apr. 25, 2018, 6:23 PM), http://perma.cc/9P2P-KH7K (discussing the valuation of large technology firms).

58. *Id.*

59. *See* Larry Dignan, *CVS Health and AETNA Bet $69 Billion Merger on Analytics, Data, Digital Transformation*, ZDNET (Dec. 4, 2017), http://perma.cc/9E9G-RZ9W (describing the advantages of the CVS and AETNA merger)

60. *See id*.

61. *Id.*

62. *See* GRUNES & STUCKE, *supra* note 56, at 42.

63. *See id*. The involvement of state attorneys general eventually convinced Radio Shack to limit the data it sold during the bankruptcy process. *See* David Munkittrick, *The Legacy of the Radio Shack Bankruptcy and the Importance of PII*, PROSKAUER (Oct. 4, 2015), https://privacylaw.proskauer.com/2015/10/articles/ftc-enforcement/the-legacy-of-the-radioshack-bankruptcy-and-the-importance-of-pii/.

Borders not to share its customers' data without their consent."[64] As both of these examples attest, the ease of onward transfer enables firms to acquire personal data while evading contractual obligations to protect it.

2. The Data Broker Industry

As with corporate transactions, data brokers exemplify both the aggregation imperative and the ease of onward transfer. Brokers "collect and maintain data on hundreds of millions of consumers, which they analyze, package and sell generally without consumer permission or input."[65] Indeed, the industry leader, Acxiom, reportedly collects information on 96% of American households.[66] In turn, brokers sell this information to a range of companies, from credit card issuers, to retail banks, to telecom/media companies.[67] For the most part, contract law governs this complex chain of transfers.[68]

The entire data broker industry is a testament to the aggregation imperative. Brokers amass data from a staggering variety of sources, typically "without direct interaction with consumers."[69] One broker tracks "over 85% of the world's [pharmaceutical] prescriptions by sales."[70] Another collects "information on more than $1 trillion on consumer spending 'across 1400+ leading brands.'"[71] Still others buy data from the "250,000 websites . . . [that] state in their privacy policy that they share data with other companies for marketing and/or risk mitigation purposes.'"[72]

To aggregate data without incurring contractual commitments to consumers, data brokers depend on the ease of onward transfer. As the Federal Trade Commission (FTC) has recognized, brokers "obtain most

64. Paul A. Chandler, *Key Privacy Issues in M&A Transactions*, MAYER BROWN (Oct. 21, 2014), https://www.mayerbrown.com/-/media/files/news/2014/10/key-privacy-issues-in-ma-transactions/files/2014-10-21-key-privacy-issues-in-ma-transactions/fileattachment/2014-10-21-key-privacy-issues-in-ma-transactions.pdf.

65. SENATE COMM. ON COMMERCE, SCI., AND TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES i (2013) [hereinafter A REVIEW OF THE DATA BROKER INDUSTRY].

66. Richard Behar, *Never Heard of Acxiom? Chances are It's Heard of You, How A Little-Known Little Rock Company—The World's Largest Processor of Consumer Data—Found Itself at the Center of a Very Big National Security Debate*, FORTUNE (Feb. 23, 2004), http://perma.cc/7ZLD-C7J5.

67. *See* A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 65, at 29.

68. *See id*. at 20.

69. *Id.* at iii.

70. AARON RIEKE ET AL., DATA BROKERS IN AN OPEN SOCIETY 8 (2016), http://perma.cc/D5DM-KNYS.

71. *Id*. at 11.

72. A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 65, at 20.

of their data from other data brokers rather than directly from an original source."[73] This complex chain of transfers makes it "virtually impossible for a consumer to determine the originator of a particular data element."[74] To "perpetuate this secrecy," many brokers "contractually limit[ ] customers [that is, companies that purchase data from brokers] from disclosing their data sources."[75] In a testament to the importance of concealing the origins of data, data brokers consistently refuse "to identify the specific sources of their data or the customers who purchase it," even when requested to do so by the Senate.[76] Without any information about how data brokers collect their data, consumers have little ability to control the dissemination of their information. In this way, the ease of onward transfer enables brokers (and the firms that supply data) to escape liability for breach of contract and other claims.[77]

3. Consumer Contracts

Every day, consumers exchange personal data for services, discounts, and sometimes even payment. Companies such as Google and Facebook offer a simple deal: "[s]how us who you really are and the digital world will be free to search or share."[78] The variety and volume of these data-for-service transactions continues to grow. For example, consider the internet of things, a term that refers to devices that "measure and monitor their environment, goods, and consumers in real time."[79] This includes products that range from Fitbits to Whirlpool's internet-connected appliances.[80] In exchange for access to new features, each device collects users' health, biometric, or location information.[81]

As above, these transactions illustrate both attributes of personal data. First, an important motivation for these exchanges is that they

73. FED. TRADE COMM'N., DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 46 (2014) [hereinafter FTC, DATA BROKERS].

74. *Id*. at 14.

75. A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 66, at iii.

76. *Id*. *See also* Angelique Carson, *At Hearing, U.S. Sens. Incredulous Data Broker Industry Didn't Show Up*, IAPP (June 12, 2019), https://iapp.org/news/a/at-senate-hearing-lawmakers-incredulous-data-brokers-a-no-show/.

77. *See infra* Part I.B.3 (explaining the growing consensus in favor of treating privacy policies as enforceable contracts between data subjects and data processors).

78. *See* David Streitfeld et al., *How Calls for Privacy May Upend Business for Facebook and Google*, N.Y. TIMES, (Mar. 24, 2018, 2:22 PM), https://www.nytimes.com/2018/03/24/technology/google-facebook-data-privacy.html.

79. Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 845 (2016).

80. *See id*. (discussing various examples of the internet of things).

81. *See id.*; Lee Rainie & Maeve Duggan, *1. The State of Privacy*, PEW RES. CTR. (Jan. 14, 2016), https://www.pewresearch.org/internet/2016/01/14/the-state-of-privacy/.

permit companies to aggregate user data. Consider store loyalty cards, which trade discounts for large volumes of data about customers' shopping habits.[82] In a similar vein, some insurers offer discounts for customers who install monitoring devices that track their driving behavior.[83] Progressive,[84] for instance, has had such a program in place since 1998.[85] Like loyalty cards, driving monitoring programs depend on aggregation. Without large data sets of driving behavior, insurers cannot distinguish dangerous drivers from diligent ones.

Second, consumer data transactions depend on the ease of transfer. In practice, "[e]ach website, financial arrangement, visit to a clinic, or new mobile app [that consumers encounter] presents its own privacy practices."[86] For the most part, courts treat privacy policies as contracts that set out the terms of exchange.[87] Because of the ease of onward transfer, nothing prevents consumers from entering into dozens of these data contracts every day. The problem with easy transfer is that consumers enter into so many transactions that they struggle to meaningfully evaluate the terms of each one.[88] As a result, "it is exceedingly easy to elicit consumers' assent to the terms. . . ."[89] Thanks to the ease of onward transfer, data processing firms set the rules, while consumers sit on the sidelines.

C. Market Failures

Through corporate transactions, purchases from data brokers, and deals with consumers, firms exchange personal data.[90] As the preceding

82. *See* Lee Rainie & Maeve Duggan, *Scenario 4: Consumer Loyalty Cards and Profiling*, PEW RES. CTR. (Jan. 14, 2016), https://www.pewresearch.org/internet/2016/01/14/scenario-consumer-loyalty-cards-and-profiling/.

83. *See* Lee Rainie & Maeve Duggan, *Scenario 5: Auto Insurance Discounts and Monitoring*, PEW RES. CTR. (Jan. 14, 2016), https://www.pewresearch.org/internet/2016/01/14/scenario-auto-insurance-discounts-and-monitoring/.

84. *Id.*

85. *Id.*

86. Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting Over Privacy: Introduction*, 45 U. CHI. J. LEGAL STUD. S1, S4 (2016).

87. *See* Oren Bar-Gill et al., *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. CHI. L. REV. 7, 28 (2017) (relying on empirical evidence to conclude that "privacy policies are typically recognized as contracts"); *but see* Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. REG. 45, 53, 85 (2019) (replicating the Bar-Gill study and finding a weaker trend towards recognizing privacy policies as contracts).

88. *See* Ben-Shahar & Strahilevitz, *supra* note 86, at S4 ("[M]ost consumer transactions are accompanied by long predrafted standard-form agreements").

89. *Id*. at S4.

90. *See* A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 65, at i.

sections hint, however, the contracts-based status quo suffers from serious shortcomings, including: (1) information costs, (2) enforcement costs, (3) insufficient incentives to supply data, and (4) insufficient incentives to safeguard data.

1. Information Costs

In theory, legal systems rely on contract law "when it is cost effective to impose a relatively large informational burden on a small number of identified people."[91] Yet contracts about personal data impose those informational burdens on *large* numbers of people.[92] To some extent, information costs pose a problem for all consumer contracts. But those costs are *particularly* steep when it comes to contracts that cover personal data.[93] Consumers trade away their personal information many times each day—perhaps more than any other asset.[94] Indeed, one study calculated that a consumer who attempted to read every privacy disclosure would spend about eight days per year doing so.[95] And, even compared with other forms of consumer contracts, "privacy rights deal with matters that are not intuitive for consumers."[96] Indeed, one experiment found that "differences in [privacy] policy language that are quite salient to lawyers are essentially irrelevant to consumers."[97] So, at least in some cases, consumers agree to exchanges that they would not have if they had understood the full details. To take just one example, consider the Cambridge Analytica scandal, in which Facebook users unwittingly supplied third-party gaming apps with information about themselves and their friends.[98] With a complete understanding of when their information would be shared with third-parties, at least some of those users presumably would have elected not to participate. The reverse is also true. Some consumers may overestimate the risks of exchanging their data. With better information about the risks, some data subjects might engage in exchanges

91. Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 790 (2001).

92. *See id*.

93. *See* A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 65, at 5–8.

94. *See* Martin, *supra* note 39.

95. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 543, 565 (2008).

96. Ben-Shahar & Strahilevitz, *supra* note 86, at S4.

97. Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 U. CHI. J. L. STUD. S69, S92 (2016).

98. *See* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

that they currently forgo. Both possibilities distort the market for personal information.

2. Enforcement Costs

None of the types of exchange described in Part I.B solve the onward transfer problem. While the cost of onward transfer approaches zero, the cost of discovering violations and then bringing legal action against the transferor is necessarily greater than zero. Accordingly, data processors can share information more easily than data subjects can stop them from doing so. So it is no surprise that the web of contracts underlying the data broker industry makes it "virtually impossible for a consumer to determine the originator of a particular data element."[99] The more difficult it is for consumers to enforce rights in their data, the easier it is for data brokers to sell that data. This helps explain why brokers forbid purchasers from "disclosing their data sources."[100] At the same time, information costs also exacerbate enforcement problems. Because consumers rarely study privacy policies, they "have little real knowledge or choice about which specific third parties may have their information and how those third parties will use and further disclose such information."[101] And even when data subjects detect unauthorized use of their data, they often have no legal recourse.[102] By definition, a system of exchange rooted in contract law only permits consumers to enforce their rights against counterparties.[103] So long as personal information can be quickly copied and shared, *in rem* rights may be necessary.

3. Incentives to Supply Personal Data

Data subjects' inability to protect their data from third-party transfers distorts their incentives to produce information.[104] Under the status quo, data subjects do not capture the social returns of supplying higher-quality data. Regardless of the quality of the data that consumers produce, they receive the same free online services as everyone else. As a result, data subjects have little incentive to supply accurate, high-quality information to data processors.[105] At first, it may seem that data subjects do

99. FTC, DATA BROKERS, *supra* note 73, at 14.

100. A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 65, at iii.

101. Asay, *supra* note 49, at 333.

102. *See id.* at 328.

103. *See* Merrill & Smith, *supra* note 91, at 776–77.

104. *See* Asay, *supra* note 49, at 326.

105. *See* POSNER & WEYL, *supra* note 29, at 232 (decrying "[t]his lack of effective incentives").

not need an incentive to create information, since they do so just by going about their lives.

But that is not always the case.[106] In practice, most consumers have refused to "provide information that isn't relevant to a transaction."[107] More problematically, 24% report giving "inaccurate or misleading information about themselves."[108] Accordingly, much of the "information about consumers obtained by data brokers may not always be correct and could be out of date."[109] By sabotaging their personal information, data subjects undermine the gains from harnessing data. Supplied with inaccurate data, algorithms will be less powerful and predictions less accurate.[110] By contrast, when "consumers play an active role in logging [that is, supplying] their data," that data "may be more accurate."[111] Over time, the demand for high-quality data is likely to grow.[112] As economists explain, "many A[rtificial] I[ntelligence] systems depend on active participation by humans to generate relevant data."[113] Big data and machine learning applications also depend on accurate data.[114] In short, by reducing data subjects' incentives to supply quality data, the status quo impedes the development of artificial intelligence, predictive algorithms, and other technologies.

106. To be sure, this means that types of data that consumers produce naturally (for example, social media posts) will be less affected by this problem. But types of data that demand active participation by consumers are becoming more important—and more common. *See infra* Part II.A.2 (discussing how AI, machine learning, and big data often require active participation by data subjects).

107. Mary Madden & Lee Rainie, *Attempts to Obscure Data Collection and Preserve Anonymity*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/attempts-to-obscure-data-collection-and-preserve-anonymity/ [hereinafter Madden & Rainie, *Attempts to Obscure Data Collection*].

108. *Id*.

109. Stacy-Ann Elvy, *Paying For Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1443 (2017).

110. And possibly discriminatory. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 684 (2016) ("Decisions that depend on conclusions drawn from incorrect, partial, or nonrepresentative data may discriminate against protected classes.").

111. Elvy, *supra* note 109, at 1443.

112. *See id.* at 1383.

113. *See* Imanol Arrieta-Ibarra et al., *Should We Treat Data as Labor? Moving Beyond "Free"*, 108 AEA PAPERS & PROC. 38, 39 (2018).

114. *See* Barocas & Selbst, *supra* note 110, at 684; POSNER AND WEYL, *supra* note 29, at 229–30 (explaining that machine learning and artificial intelligence depend on large quantities of data, and that the returns to data are increasing rather than decreasing).

4. Incentives to Safeguard Personal Data

Data processors reap the benefits of personal information, but they do not bear the full risk when that information is compromised. After a data breach, individuals face identity theft, but data processors do not. And the fate of identity theft victims is grim.[115] One author explains that victims "may be forced to file for bankruptcy . . . [t]heir utilities may be cut off and their services denied . . . [and] their stolen health information may be used to obtain medical care, saddling them with hefty hospital bills and a thief's treatment records."[116] According to one estimate, the "average cost of repairing identity theft was $1,769, and the median loss was $300."[117] To be sure, breach notification laws and other regulatory responses encourage companies to safeguard data. But, judging by the steadily increasing number of data breaches, the results of these policies are mixed.[118] Take Wyndham Worldwide, a hotel chain, which experienced three consecutive data breaches due to its use of default passwords and lack of firewalls.[119] Notice, too, that data breaches magnify the enforcement challenges described above. After all, breaches result in more copying and sharing of personal information, making it even harder for consumers to monitor their information and vindicate their rights.

From this overview of the status quo, two themes emerge. First, the essential attributes of personal data—its sensitivity to aggregation and its susceptibility to onward transfer—shape the contours of personal data markets.[120] Second, the contracts-based status quo suffers from multiple market failures.[121] The volume and variety of contracts impose prohibitively high information costs, limiting data subjects' ability to understand the exchanges they participate in.[122] And, because contract rights are *in personam* rather than *in rem*, data subjects struggle to enforce their interests against subsequent purchasers.[123] Thanks to high information and

115. *See* Alessandro Acquisti, *The Economics of Personal Data and the Economics of Privacy* 16 (Nov. 24, 2010) (unpublished manuscript) (on file with author) ("[V]ictims can suffer a ruined credit score, inability to access credit or employment, or even criminal charges. . . .").

116. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 756–57 (2018).

117. *Id*. at 757.

118. *See* Chris Morris, *Hackers Had a Banner Year in 2019*, FORTUNE (Jan. 28, 2020, 11:15 AM), https://fortune.com/2020/01/28/2019-data-breach-increases-hackers/ (reporting that there were 1,473 data breaches in 2019, 18% more than in 2018).

119. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241–42 (3d Cir. 2015).

120. *See supra* Part I.A.

121. *See supra* Part I.B.3.

122. *See supra* Part I.C.1.

123. *See supra* Part I.C.2.

enforcement costs, the status quo both smothers data subjects' incentive to supply high-quality data and suppresses data processors' incentive to safeguard that data.[124] In keeping with Demsetz's emphasis on "the gains from internalization," Part II asks whether property rights can rectify these market failures.[125]

II. THE PROMISE OF PROPERTY RIGHTS

For decades, economists have recognized that propertization can be a powerful tool to address market failures.[126] Indeed, Harold Demsetz even defined property rights as laws that enable market exchange.[127] Despite the link between property rights and thriving markets, however, the common law has so far declined to treat personal data as property.[128] This Part asks whether creating property rights in personal data promises to improve on the status quo.[129]

The answer is yes. Though propertization is not a panacea, extending property rights would mitigate each of the market failures that plague personal data markets. Under this system, property law would not displace contract law altogether. Instead, contracts and property would coexist, as they currently do with respect to sales of land, for example. Adding property rights to the contracts-based status quo promises to reduce information and enforcement costs while aligning data processors' and data subjects' incentives.

To be sure, extending property rights may resolve existing market failures only to create new ones. In theory, propertization may exacerbate behavioral biases, undermine privacy as a public good, and demand unrestricted alienability of data.[130] In practice, however, these problems

124. *See supra* Parts I.C.3 & I.C.4.

125. Demsetz, *supra* note 5, at 348.

126. *See, e.g.*, DARON ACEMOGLU & JAMES A. ROBINSON, WHY NATIONS FAIL: THE ORIGINS OF POWER, PROSPERITY, AND POVERTY 429–30 (2012) (arguing that property rights are an essential tool to foster economic growth).

127. *See* Demsetz, *supra* note 5, at 350. "An owner of property rights possesses the consent of fellowmen to allow him to act. . . ." *Id.* at 347.

128. *See* Samuelson, *supra* note 14, at 1131 (observing that "the traditional view in American law has been that information as such cannot be owned by any person"). For an example of litigants (unsuccessfully) arguing in favor of treating personal information as property, *see* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 695 (7th Cir. 2015) (noting that "[p]laintiffs refer us to no authority that would support" finding that personal information is property).

129. *See supra* Part I.B.

130. Because that debate reached its apex about 15 years ago, its discussion of the status quo no longer reflects existing technologies and markets. For the most detailed discussion of the status quo, *see* Schwartz, *supra* note 15, at 2084 (condemning "nirvana fallacies" that

apply with equal or greater force to the status quo. As a result, extension of property rights is unlikely to make these problems any worse than they already are. Ultimately, comparing the contract-based status quo with a hypothetical property regime confirms that the gains from propertization—the first half of Demsetz's formula—may be significant.

A. The Case for Propertization

This Section argues that extending property rights in personal data would improve on the status quo. At the outset, it is necessary to clarify "a notoriously nebulous concept"—property.[131] This Article defines property as any legal regime that incorporates three elements.[132] First, property grants a bundle of rights, including rights to exclude, use, transfer, and destroy.[133] Second, those rights are good against the world (*in rem*), rather than limited to specific counterparties (*in personam*).[134] Third, that regime must limit property owners' ability to alienate property rights. To be clear, this is not an essential element of all property regimes, but it is essential to protect property rights in personal data.[135]

Armed with this definition of property, this Section revisits the four market failures that Part I identified: (1) high information costs, (2) high enforcement costs, (3) insufficient incentives to supply information, and (4) insufficient incentives to safeguard information. Extending property rights in personal data promises to alleviate each of these problems.

1. Information Costs

Scholars recognize that one of the primary virtues of propertization is that it reduces information costs, especially when the volume of transactions is high.[136] As Henry Hansmann explains, property law "defines a set of well-recognized forms that property rights can take . . . ."[137]

focus only on idealized versions of reality). In that 2004 paper, Schwartz discussed implantable chips, compensated telemarketing, and other technologies that have not (yet) taken root.

131. *See* Jacob M. Victor, Comment, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 518 (2013).

132. *See* Schwartz, *supra* note 14, at 2058 (defining "property as any interest in an object, whether tangible or intangible, that is enforceable against the world").

133. *See* Merrill, *supra* note 21, at 730–39 (discussing the theory of property as a bundle of rights).

134. *See* Schwartz, *supra* note 14, at 2058.

135. Section II.B.3 explains why this is so.

136. *See* Merrill & Smith, *supra* note 92, at 793 ("[I]n rem rights . . . conserve on information costs . . . where the number of potential claimants on resources is large, and the resource in question can be defined at relatively low cost.").

137. Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. 373, 373 (2002).

Thomas W. Merrill and Henry E. Smith concur, noting that those rights are "standardized and immutable, and focus on gross proxies . . . that are easy to observe and grasp by a large and heterogeneous population . . . ."[138] The more standardized property rights are, the lower the information costs required to assess a proposed exchange.[139] In general, standards conserve information "by making . . . duties apply automatically to delineated resources without regard to the identity of the owner; by making the duties uniform; [and] by restricting the duties to a short list of negative obligations . . . ."[140]

Today, consumers face an unappealing choice: either spend eighty days a year reading every privacy policy, or ignore those policies and remain ignorant of the details of each exchange.[141] Imagine instead that personal data always carried the same bundle of rights.[142] That bundle might include the rights to exclude, transfer, destroy, and use—the traditional rights associated with property.[143] But the specific rights in the bundle do not matter, at least for the purpose of reducing information costs. What does matter is that the *same* bundle always accompanies personal data. So long as data subjects understand that standard bundle, they will rarely need to examine privacy policy language. As a result, data subjects would understand the property interest transferred when they use websites—without reviewing hundreds of privacy policies.[144]

Beyond that, propertization could reduce information costs for third-party data purchasers. As Alvin Roth explains, standardization enables market designers to transform "a market into a commodity market [which] make[s] it really thick."[145] When data brokers seek to buy data, or an acquiring company purchases a start-up for its data, they would no longer need to investigate the specific contractual promises made to each

138. Merrill & Smith, *supra* note 91, at 852.

139. *See id.* at 843.

140. *Id*. at 794.

141. *See supra* Part I.C.1 (explaining that information costs are particularly steep when applied to information contracts).

142. It is tempting to argue that regulators could achieve the same result by mandating a standard set of contractual terms. But, at least in the case of personal data, such a regime would need to be accompanied by *in rem* rights. Otherwise, data processors could sell consumer data to data brokers, evading the standard contractual terms. *See supra* Part I.B.2 (introducing the data broker industry). In other words, for such a contract regime to work, it would likely need to look very similar to a property regime.

143. *See infra* Part III.B (discussing how GDPR installs these rights).

144. *See* McDonald & Cranor, *supra* note 95, at 565.

145. ALVIN E. ROTH, WHO GETS WHAT—AND WHY: THE NEW ECONOMICS OF MATCHMAKING AND MARKET DESIGN 17 (2015).

data subject.[146] Instead, they will understand that every data subject has the same bundle of rights. The easier it is for data purchasers to know exactly what rights they are receiving when they buy data, the thicker the market.

Standards do have a downside. Unlike the default rules in contract law, standards thwart the creation of non-standard bundles of rights. Merrill and Smith coined the term "frustration costs" to describe the expenses market participants encounter when they cannot customize the bundle of rights attached to an asset.[147] But extending property rights does not foreclose customization altogether. While contracts cannot modify the standard bundle of rights, they can provide additional promises.[148] At the same time, when it comes to personal data, frustration costs are likely to be small relative to the benefits of reducing information costs. Because market participants exchange an enormous amount of personal data, and because those transactions involve relatively low value data, data subjects are unlikely to place a premium on customization.[149] Thus, frustration costs almost certainly pale in comparison with the benefits of reducing information costs across millions of personal data transactions.

2. Enforcement Costs

Propertization facilitates enforcement in two ways. First, *in rem* rights enable enforcement against data processors who are currently beyond the reach of contract law. That is, propertization "renders every processor of the personal data liable, regardless of their relation to the data subject, allowing consumers to control the spread of their sensitive personal information . . . ."[150] Take data brokers. So long as brokers avoid contractual commitments to data subjects, they have little reason to fear breach of contract claims.[151] As such, a contracts regime helps insulate brokers from liability.

Under an *in rem* regime, by contrast, data subjects would be able to bring legal claims against data brokers—regardless of whether those

146. Compare this with the current market, where every website policy is infinitely flexible. *See supra* Part I.C.1 (noting that contracts about personal data impose informational burdens).

147. *See* Merrill & Smith, *supra* note 91, at 797.

148. *See id*. at 850 (stating that, in their purest form, property rights involve "immutable bright-line rules"). *See also* Part III.C (describing that GDPR makes the standard bundle of rights in personal data immutable by preventing data subjects from alienating those rights).

149. *See supra* Part I.A.1 (discussing that volume distinguishes personal data from other assets).

150. Hertza, *supra* note 15, at 1739.

151. *See supra* Part I.B (explaining that the marketplace has evolved in a manner that affects every consumer and organization).

brokers have breached any contractual commitments.[152] For this to work, data subjects cannot be permitted to alienate their property rights unconditionally. Otherwise, data processors could convince data subjects to forfeit their rights through contract, essentially undoing the propertization regime.[153] Another caveat is that granting data subjects rights against the world is not the same as creating institutions that ensure effective enforcement of those rights. Part IV takes up that question.

Second, property rights provide an alternative enforcement mechanism that may sometimes be more powerful than breach of contract claims. In describing how intellectual property rights facilitate commercial transactions, Robert P. Merges has explained that property rights offer "enforcement flexibility."[154] One advantage of bringing a property claim is that the litigation costs to enforce property rights may be lower than those required to show that a data processor violated a contractual obligation.[155] As scholars recognize, contract interpretation generally involves "costly litigation with unpredictable outcomes."[156]

Another advantage is that courts may be more willing to grant injunctions as a remedy for violations of property rights than for breaches of contract.[157] This might reduce expensive litigation necessary to measure damages. Of course, property rights do not completely replace breach of contract claims. In some cases, contracts include additional promises that go beyond property rights. As Merges observes, property rights improve "enforcement flexibility" by *complementing* contract claims, rather than *substituting* for them entirely.[158] Because aggrieved parties can bring either contract or property claims, propertization increases the overall likelihood of successful enforcement.

To be clear, property does not promise to solve every enforcement challenge. To take one example, data subjects may still struggle to detect whether data processors are respecting their property rights in the first place. So, while *in rem* rights, lower litigation costs, and a broader range

152. *See* Hertza, *supra* note 15, at 1739.

153. *See* Part II.B.3 (explaining the limited alienability requirement).

154. *See* Robert P. Merges, *A Transactional View of Property Rights*, 20 BERKELEY TECH. L. J. 1477, 1485, 1487 (2005) (observing that "property rights substantially enhance the enforcement options of contracting parties, through a collection of discrete rules and doctrines").

155. *See id.* at 1506.

156. *See* Omri Ben-Shahar & Lior Jacob Strahilevitz, *Interpreting Contracts Via Surveys and Experiments*, 92 N.Y.U. L. REV. 1753, 1761 (2017) (noting that "[e]xisting interpretation doctrines are difficult to apply and lead to costly litigation with unpredictable outcomes").

157. *See* Anthony T. Kronman, *Specific Performance*, 45 U. CHI. L. REV. 351, 354 (1978) (explaining that "[t]he normal remedy for breach of contract is, of course, money damages [and s]pecific performance is exceptional").

158. *See* Merges, *supra* note 154, at 1485.

of remedies offer higher odds of success, they do not provide a complete solution.

3. Supplying and Safeguarding Data

Enhanced enforcement aligns data processors' and data subjects' incentives. Data processors want data subjects to supply high-quality data.[159] And data subjects want data processors to safeguard their data.[160] *In rem* enforcement improves the odds of both outcomes.

For one thing, though critics of propertization maintain that "[c]ompanies hardly seem to need any further incentives to continue hoarding data,"[161] extending property rights promises to improve the quality of data, if not its quantity. One way to understand this is in terms of trust, a key ingredient for successful markets. As Alvin Roth explains, "for a market to be truly trustworthy, it must be safe; participants on both sides of a transaction must be able to rely on each other and on the technology."[162] Under the status quo, all that data processors need to do to avoid contractual commitments is to sell data to a broker.[163] As a result, some data subjects lose trust in the market, even going so far as destroying or "pollut[ing]" their data.[164] Improved enforcement discourages destructive self-help. The more that consumers trust that firms will be held to their commitments, the less likely they are to provide false and misleading data. In short, creating property rights may correct "a lack of self-interested incentives for a particular stakeholder group to make its data available."[165]

159. *See* Jiahong Chen, *The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle*, 4 EUR. DATA PROTECTION L. REV. 36, 36 (2018).

160. *See* Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, CONSUMER REP. (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data/.

161. Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 35 (2018).

162. ROTH, *supra* note 145, at 116.

163. *See supra* Part I.B.2 (discussing how data brokers depend on ease of transfer among each other to maintain data secrecy).

164. *See, e.g.*, Lil Miss Hot Mess, *A Drag Queen's Guide to Protecting Your Privacy on Facebook by Breaking the Rules,* WIRED (Apr. 3, 2018, 9:00 AM), http://perma.cc/SXQ6-GD46 (urging consumers to use a false name on social media, tag photos incorrectly, and deploy other methods to protect their information). *See also* Julia Powles, *Obfuscation: How Leaving a Trail of Confusion Can Beat Online Surveillance*, THE GUARDIAN (Oct. 24, 2015, 4:00 PM), http://perma.cc/H4VD-6A7R (recommending "the addition of ambiguous, confusing, or misleading information to interfere with surveillance"); Madden & Rainie, *Attempts to Obscure Data Collection*, *supra* note 109 (noting that 24% of consumers report giving inaccurate information about themselves).

165. *See* JAMES MANYIKA ET AL., *supra* note 30, at 118.

For another thing, improved enforcement encourages data processors to safeguard the personal data that they store. The more likely that data subjects will recover damages after a data breach, the more that data processors will invest in cybersecurity defenses that reduce the risk of a breach in the first place. So stronger enforcement prompts data subjects to supply high-quality data, while simultaneously encouraging processors to invest in cyber security.

Table 1: How a Property Regime Compares with the Status Quo

Feature	Status Quo	Property Regime
Information Costs	Relatively high; data subjects must review a potentially infinite array of contractual terms	Relatively low; the standard bundle of property rights limits the permissible range of contractual terms[166]
Enforcement Costs	Relatively high; data subjects struggle to enforce rights against subsequent transferees (e.g., brokers)	Relatively low; rights are *in rem*, and data subjects can enforce their rights through either contract or property
Data Quality	Relatively low; data subjects have little incentive to supply accurate, high-quality data	Relatively high; increased trust discourages data subjects from "polluting" their data
Data Security	Relatively low; ineffective enforcement means that data processors have insufficient incentive to invest in safeguards	Relatively high; more effective enforcement means that data processors have an incentive to invest in safeguards

Table 1 compares a property regime—including a bundle of *in rem* rights—with the status quo.[167] Property rights promise to reduce information costs and amplify the odds of successful enforcement.[168] However, it may be that property rights address the problems associated with

166. One possible objection is that, if data subjects and data processors retain the ability to form contracts, the menu of options is not limited. The solution depends on inalienability. So long as data subjects cannot alienate property rights through contract, regulators can limit the menu of options. *See* Part II.B.3 (discussing the alienability requirement). GDPR adopts this approach, which Paul M. Schwartz calls "hybrid inalienability." *See* Schwartz, *supra* note 14, at 2060.

167. Again, for more specifics about what this bundle includes, and about how *in rem* rights in personal data would function, *see infra* Part III (describing how GDPR accomplishes both of these functions).

168. This idea has received remarkably little attention. *See* Merges, *supra* note 154, at 1479 ("With some exceptions, commentators continue to analyze and discuss property and contract as opposing concepts and quite distinct legal categories.").

the status quo only to create a different set of challenges. The next Section raises—and then rejects—that possibility.

B. The Exaggerated Pitfalls of Propertization

This Section asks whether extending property rights in personal data will address existing market failures only to produce new, unintended consequences. Critics warn that propertization will exacerbate behavioral biases, undermine privacy's status as a public good, and amplify the alienability of information.[169] But, because these problems apply with equal or greater force to the status quo, none threatens the appeal of extending property rights in personal data.

1. The Problem of Information Asymmetries

One of the most common concerns about propertization proceeds in two steps. The first step observes that information asymmetries plague exchanges of personal data.[170] For example, the value of data depends on aggregation, and only data processors know how data will be combined.[171] Because data subjects struggle to foresee future risks, they may give away data too easily.[172] The second step predicts that extending property rights in personal data will encourage consumers to think of it as a commodity, prompting more exchanges that suffer from information asymmetries.[173]

This logic falters at the second step. Under the status quo, consumers exchange enormous volumes of personal data.[174] Behavioral biases already play a role in those transactions.[175] It is far from obvious that more data would be exchanged under a property regime. While property rights

169. *See* Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 748 (2004) ("Exceptions to the norm of alienability may exist, but these norms nevertheless push objects of property toward commodification.").

170. *Need for Internet Privacy Legislation: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 107th Cong. 33 (2001) (statement of Paul M. Schwartz, Professor of Law, Brooklyn Law School).

171. *See supra* Part I.A.1 (discussing that volume distinguishes personal data from other assets).

172. *See* Solove, *supra* note 46, at 1881.

173. *See, e.g.*, Determann, *supra* note 161, at 37–38 ("[I]f data can be sold, licensed, and traded like commodities, this would inevitably have negative effects on the protection of personal privacy.").

174. *See supra* Part I.B (discussing the volume of data in the current market).

175. *See generally* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES (Alessandro Acquisti et al. eds., 2008) (cataloging the information asymmetries inherent in exchanges of personal information).

permit data subjects to *transfer* data, they also protect the right to *exclude* others from accessing that data.[176] As important, in a property regime, exchange would be based on standard bundles of rights,[177] which reduce information costs and enable consumers to assess the risks associated with each exchange.[178] So, while propertization does not address information asymmetries entirely, it does promise at least a modest improvement over the status quo.

2. The Public Goods Problem

A second argument against property rights depends on a concept that this Article has not yet discussed: privacy.[179] Critics of propertization explain that protecting personal information has societal benefits that exceed the benefit to any one individual.[180] Put in economic terms, privacy is a public good.[181] In theory, when individuals protect their privacy, they become more creative, diverse citizens.[182] In turn, diversity and creativity benefit the public as a whole.[183] Proponents of this argument caution that property rights in personal data will not account for these benefits, leading to underinvestment in privacy.[184]

Once again, the fundamental problem with this argument is that it ignores the status quo. The right to exclude enables data subjects to keep more of the social benefits of their data than they do today. So the public

176. *See* Merrill, *supra* note 21, at 743 ("[T]he ordinary understanding is that a person who has the right to exclude also is presumed to have the right to transfer. It takes some special conveyance or legislation to defeat the expectation that the right to exclude entails a right to transfer.").

177. For specifics on the rights that would be included in this bundle, *see infra* Part III.B (describing the property rights that GDPR associates with personal data, including the right to exclude, use, transfer, and destroy).

178. *See supra* Part II.A.1 (explaining the benefits of propertization).

179. The reason that I use the term privacy sparingly is because it is so difficult to define. In general, privacy has something to do with personal information, but different authors have different ideas about what that "something" is. By referring to personal information throughout this Article, I have attempted to be more precise about the interests at stake.

180. *See generally e.g.*, Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMM. TECH. L. REV. 367 (2012) (arguing against the propertization of personal information).

181. Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 387 (2016).

182. *See* Julie E. Cohen, *Privacy and Technology: What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013).

183. *See* Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1427 (2000) (arguing that "[i]nformational privacy . . . is a constitutive element of a civil society in the broadest sense of that term").

184. *See* Schwartz, *supra* note 14, at 2084–90 (summarizing arguments about privacy as a public good).

goods hypothesis suggests that property rights are a step in the right direction—given that individuals would capture greater returns from their data—though not a complete solution. But property rights need not occupy the entire field of privacy regulation. To account for privacy's status as a public good, regulators could develop laws that forbid information exchange in certain domains. In fact, many countries protect children's data[185] as well as data about adults' political affiliation.[186] In both cases, regulators protect the data that is most essential to nurturing diverse, creative citizens. Because propertization cannot solve every privacy problem, legislators remain free to marry a property rights regime with additional protections.

3. The Alienability of Property Rights

Finally, some skeptics equate property rights with unlimited alienability.[187] Given the ease of onward transfer, a legal regime that guaranteed complete alienability of personal data would be no better than the current contract regime. Under that approach, a data subject could sign away all of her property rights to a data processor. Then, the processor could share that data with third parties, putting it beyond the data subject's control.[188] In other words, unlimited alienability would permit data processors to permanently divest data subjects of property rights.

But this result only follows if alienability is an essential feature of property. It is not.[189] In fact, the common law often limits alienability. For instance, when landowners are unable to sell their land, the common law forbids them from abandoning it.[190] In a similar vein, state and local ordinances often restrict owners' ability to alienate lots of a particular size.[191] These examples suggest that, when it comes to traditional forms of property, alienability need not be absolute. The same is true for property in personal data. As Paul M. Schwartz has observed, it is possible to

185. *See, e.g.*, Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2020).

186. *See e.g.*, GDPR, *supra* note 1, Recital 75.

187. Pamela Samuelson is the leading proponent of this approach. *See* Samuelson, *supra* note 14, at 1137–38 (observing that "[c]hief among [the objections to propertization] is the difficulty with alienability of personal information").

188. *See supra* Part I.B (discussing personal data markets and consumer contracts).

189. *See, e.g.*, Schwartz, *supra* note 14, at 2090–94 (demolishing this argument in detail).

190. *See generally,* Lior Jacob Strahilevitz, *The Right to Abandon*, 158 U. PENN. L. REV. 355 (2010) (detailing various common law limitations on the right to abandon property).

191. *See, e.g.*, *Murr v. Wisconsin*, 137 S. Ct. 1933, 1940 (2017) (observing that "the Wisconsin rules prevent the use of lots as separate building sites unless they have at least one acre of land suitable for development").

imagine a property regime that involves "hybrid inalienability."[192] That regime would guarantee data subjects certain rights even after transferring a property interest in their information to a data processor.[193] This is not just a matter of theory. As Part III demonstrates, the General Data Protection Regulation (GDPR) adopts Schwartz's approach by guaranteeing that data subjects cannot waive rights in their data.[194]

The overall picture, then, suggests that extending property rights in personal data would improve the status quo. Not only would propertization address the problems associated with contracts-based exchange, but it would raise few new problems. That is not to say, however, that propertization would result in a perfect market for personal data. With property rights as a floor, regulators must account for the public goods nature of privacy.

But an essential question remains unanswered: how feasible is it to extend property rights to personal data? Demsetz recognized that the "gains of internalization," must be compared with the cost of securing property rights.[195] Contemporary scholars agree that propertization is "not costless."[196] When it comes to data, protecting property rights has the potential to be particularly expensive. Consider the attributes of personal data: it is high-volume, context-dependent, and vulnerable to onward transfer.[197] Each attribute suggests that securing personal data may require costly institutional investments. In addition, there are significant transition costs associated with implementing a system of property rights for the first time.[198] In other words, the hard question is not whether propertization offers substantial gains, but whether there is a way to capture those gains without incurring disproportionate costs. Two decades ago, Pamela Samuelson observed that, "[t]oo little thought has been given as yet to how to move from where we are today to a thriving market in personal data under a property rights regime."[199] That remains true today.

192. *See* Schwartz, *supra* note 14, at 2060.

193. *See id*. at 2094.

194. For a discussion of this approach, *see infra* Part III.B (discussing GDPR's limitation on the ability of data subject's ability to alienate their rights).

195. *See* Demsetz, *supra* note 5, at 350.

196. *See* Samuelson, *supra* note 14, at 1137. *See also* Merrill, *supra* note 21, at 733.

197. *See supra* Part I.A (discussing the features that distinguish personal data from other forms of data).

198. *See infra* Part IV.C.3 (discussing the costs of transitioning property rights in personal data).

199. Samuelson, *supra* note 14, at 1137. Similarly, Schwartz recognized the need for institutions "to provide trading mechanisms (a 'market-making' function), to verify claims to propertized personal data (a verification function), and to police compliance with agreed-upon

By examining the institutions necessary to secure property rights, the remainder of this Article seeks to fill that gap.

III. THE GENERAL DATA PROTECTION REGULATION AS PROPERTIZATION REGIME

The European Union's General Data Protection Regulation (GDPR), which came into effect in 2018, promises to revolutionize how organizations treat personal data.[200] As scholars observe, GDPR "represent[s] without any doubt the most important legal source for data protection."[201] That Regulation is relevant here because it installs a property regime for personal data.[202] The enactment of GDPR—and the proliferation of its approach—affirms that the gains from extending property rights in personal data are increasingly apparent.[203] At the same time, the Regulation offers a framework for examining the institutional costs of securing property rights, the second half of Demsetz's formula. This Part introduces GDPR's basic structure, while Part IV uses GDPR to investigate the costs of protecting rights in personal data.[204]

A. GDPR Basics

This Section summarizes GDPR's purpose, terminology, and mechanics. Importantly, the Regulation does not reflect a policy judgment that property rights in personal information are normatively desirable.[205] Rather, GDPR derives from Europe's longstanding commitment to

terms and legislatively mandated safeguards (an oversight function)." Schwartz, *supra* note 14, at 2110.

200. *See* GDPR, *supra* note 1, Recital 1 (stating that the "protection of natural persons in relation to the processing of personal data is a fundamental right"); *id.* art. 99(2).

201. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1168 (6th ed. 2018).

202. Other authors have recognized this, some more explicitly than others. *See generally* Victor, *supra* note 133 (arguing that property-based safeguards are present in GDPR, even though it is not framed in property terms); Hertza, *supra* note 15, at 1738 ("The GDPR introduces a property interest in personal data."). *See also* POSNER & WEYL, *supra* note 29, at 245 ("Governments would have to ensure that individual digital workers have clear *ownership rights over their data*, a step the European Union has moved toward with its General Data Protection Regulations.") (emphasis added); Ibarra et al., *supra* note 113, at 4 ("[N]ew regulatory frameworks such as the European General Data Protection Regulations are increasingly shifting *ownership rights in data* to the users who generate them.") (emphasis added).

203. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 122 (2017).

204. *See* Demsetz, *supra* note 5, at 350.

205. *See* GDPR, *supra* note 1, Recital 4 (stating that the "right to the protection of personal data is not an absolute right").

enshrining privacy as a human right.[206] Indeed, European Union's Human Rights Charter includes privacy among the pantheon of human rights.[207] In recognition of the importance of privacy, GDPR sets out many regulatory requirements. GDPR regulates data processors' internal operations,[208] collection consent from data subjects,[209] and installs new forms of regulatory oversight.[210] Because GDPR pursues many objectives, it should be no surprise that it implements propertization imperfectly.[211]

The Regulation distinguishes between three types of participants in the data economy. First, *data subjects* are individuals "who can be identified, directly or indirectly" using certain information.[212] GDPR endows data subjects with a set of rights, discussed in Part III.B below.[213] Second, *data controllers* "determin[e] the purposes and means of the processing of personal data."[214] However, GDPR recognized that controllers often do not process data directly, but instead rely on third-parties to do so.[215] So, finally, the Regulation covers *data processors*, who perform operations "on personal data or sets of personal data" at the direction of the

206. *See* Schwartz & Peifer, *supra* note 203 at 123–27 (describing the history of Europe's treatment of privacy as a human right).

207. *See* Human Rights Act 1998 c. 42 art. 8 (UK). The Charter provides for several limits on this broad right, including "national security, public safety or the economic well-being of the country" as well as "the prevention of disorder or crime," "protection of health or morals," and "protection of the rights and freedoms of others." *Id.* § 2.

208. *See, e.g.*, GDPR, *supra* note 1, art. 35 (requiring data processors to conduct internal "data protection impact assessments" for projects that pose privacy risks); *id.* art. 37 (directing controllers and processors to designate a "data protection officer" in certain circumstances).

209. *See, e.g.*, *id.* art. 7 (laying out a series of requirements for securing valid consent from data subjects).

210. *See, e.g.*, *id.* art. 77 (permitting data subjects to file complaints with national regulators); *id.* art. 79 (permitting data subjects to file complaints with European courts).

211. *See* discussion infra Part IV.C.5 (providing an example of how GDPR's privacy objectives sometimes undermine property rights).

212. GDPR, *supra* note 1, art. 3(1) ("[P]ersonal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.").

213. *See* discussion *infra* Part III.B.2 (explaining that rights under GDPR do not require a contractual relationship).

214. GDPR, *supra* note 1, art. 3(8). The statute embraces a broad understanding of processing, which includes "collection, recording, organization, structuring, storage . . . or otherwise making available, alignment or combination, restriction, erasure or destruction." *Id.* art. 3(2).

215. *See id.* ("'[C]ontroller' means the competent authority which, alone or jointly with others . . . .").

controller.[216] In this way, GDPR's terminology reflects the complex patterns of exchange that characterize the data economy.[217]

Before going further, it is important to emphasize the limits of GDPR's scope. The Regulation only applies to information that is processed "wholly or partly by automated means" or "which form[s] part of a filing system."[218] Suppose that you meet a friend for lunch and notice that he is wearing a yellow shirt. That knowledge is not part of a filing system, so it is not regulated by GDPR. Now imagine that you return home, download the picture onto your computer's hard drive, and give it the title, "John Doe in a Yellow Shirt." Although the picture is now part of your computer's filing system, GDPR exempts data processing "by a natural personal in the course of a purely personal or household activity."[219] Finally, suppose that a police officer snaps a picture of John Doe, hoping to prove that John stole the shirt. Can John exercise his right to exclude by demanding that the police department delete the picture? Again, the answer is no. The Regulation exempts processing for law enforcement and national security purposes.[220] The bottom line is that GDPR only covers records, with exceptions for household and law enforcement use. With these basics in mind, the next Section shows how GDPR grants property rights in personal data.

B. GDPR Creates Property Rights

In essence, GDPR grants EU citizens property rights in the data they create. To be sure, the Regulation's drafters did not set out to extend property rights in personal data.[221] But that is what GDRP accomplishes. In keeping with the definition of property elaborated in Part II, the Regulation provides data subjects with: (1) a bundle of rights[222] (2) that are good against the world[223] (3) and that data subjects cannot completely alienate.[224] The following Sections demonstrate how GDPR constructs each of these elements.

216. *See* GDPR, *supra* note 1, art. 4(2).

217. *See supra* Part I.B (discussing corporate data transactions, data brokers, and the consumer-side of the data economy).

218. GDPR, *supra* note 1, art. 2(1).

219. *Id.* art. 2(2)(c).

220. *See id.* art. 2(2)(d).

221. *See id*., Recital 2 ("This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.").

222. *See infra* Part III.B.1.

223. *See infra* Part III.B.2.

224. *See infra* Part III.B.3.

1. GDPR Duplicates the Bundle of Rights Associated with Property

For the most part, scholars associate property with a standard bundle of rights that includes rights to exclude, transfer, destroy, and use.[225] Of those, the right to exclude is the widely recognized as the most important.[226] GDPR extends rights that closely parallel the standard bundle:[227]

The right to exclude. Article 17 of the Regulation authorizes data subjects to obtain erasure of their data "without undue delay."[228] Data subjects can exercise this right whenever data controllers base processing on consent.[229] Article 21 reinforces the right to exclude by empowering data subjects "to object . . . at any time to processing of personal data concerning him or her."[230] When data subjects object, they can compel data controllers and processors to erase their data.[231] Controllers only escape this erasure requirement if they have a "compelling legitimate ground."[232] GDPR does not spell out the scope of this exception, but does offer the "exercise or defense of legal claims" as one example of a "compelling legitimate ground."[233] This limited exception does not undermine the right to exclude. After all, the common law does not provide absolute protection of the right to exclude intruders from real property.[234] Together, Articles 17 and 21 empower data subjects to exclude others from their data—by compelling them to erase it if necessary.

225. *See* Merrill, *supra* note 21, at 735–37. *See also* Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (observing that "the right to exclude others" is "one of the most essential sticks in the bundle of rights that are commonly characterized as property").

226. *See* Merrill, *supra* note 21, at 738, 740 (commenting on "the primacy of the right to exclude").

227. *See* Victor, *supra* note 131, at 524–25 (arguing that a draft version of GDPR created property rights because the data subject rights "run with" the data and that include "property-rule-based remedies"). This brief analysis did not discuss the specific rights granted by GDPR, perhaps because it focused on a 2012 draft of the Regulation.

228. GDPR, *supra* note 1, art. 17(1).

229. *See id.* art. 17(1)(b). Processing can occur without consent when processing is necessary for compliance with some other legal regime, or when it is in the "vital interests" of the data subject. *See id.* art. 6(1)(d). Guidance from the UK Information Commissioner's Office suggests that the term "vital interests" is narrow in scope and "generally only applies to matters of life and death." *See Vital Interests*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/ (last visited May 27, 2020).

230. GDPR, *supra* note 1, art. 21(1).

231. *See id.* art. 17(1)(c).

232. *See id.* art. 21(1).

233. *Id.*

234. *See, e.g.*, State v. Shack, 277 A.2d 369, 374 (N.J. 1971) (holding that non-profit workers may enter private land to aid migrant field workers).

The right to transfer. Article 20 authorizes data subjects "to transmit [their] data to another controller without hindrance."[235] To facilitate technically complex transfers, Article 20 even affords data subjects "the right to have . . . personal data transmitted directly from one controller to another."[236] What is more, the UK Information Commissioner's Office (ICO) acknowledges that Article 20 aims to effectuate transfer.[237] Indeed, the ICO hopes that Article 20 will "enable[consumers] to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits."[238]

The right to destroy. The erasure right extended by Article 17 necessarily involves the power to destroy personal data.[239] Recognizing that information may be stored in multiple places, GDPR requires processors to notify other entities that hold the same information.[240] Under Article 17, data processors have an obligation to aid in this destruction by "tak[ing] reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."[241] In this way, GDPR ensures that *all* copies of personal data are destroyed.

The right to use. Multiple aspects of GDPR enshrine data subjects' right to use their data. Article 15 guarantees access to "a copy of the personal data undergoing processing."[242] Indeed, GDPR arguably exceeds the traditional right to use by giving data subjects an inalienable right to monitor how others are using their data. For instance, when processors use "automated decision-making" to analyze data, such as "profiling," data subjects have the right to "meaningful information about the logic involved."[243]

235. GDPR, *supra* note 1, art. 20(1). The processing must be carried out by automated means and have been initially based on consent. *Id.* art. 20(1)(a), (b).

236. GDPR, *supra* note 1, art. 20(2).

237. *See Right to Data Portability*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (last visited May 27, 2020) [hereinafter "ICO"].

238. *Id.*

239. *See* GDPR, *supra* note 1, art. 17(1) (allowing the data subject to obligate the controller to erase the subject's personal data without undue delay).

240. *See id.* art. 17(2).

241. *Id.* (limiting this requirement by instructing controllers to "take[e into] account of available technology and the cost[s] of implementation").

242. *Id.* art. 15(3).

243. *See* GDPR, *supra* note 1, art. 13(2)(f).

In short, GDPR grants data subjects each of the rights commonly associated with property.

2. GDPR Grants In Rem Rights

The Regulation also affords data subjects rights against the world, not rights that are limited to a particular contractual relationship. Several provisions of GDPR illustrate this approach. Article 17, which grants data subjects the right to exclude, requires that "the controller . . . take reasonable steps . . . to inform [other] controllers which are processing the personal data that the data subject has requested the erasure . . . of any links to, or copy or replication of, those personal data."[244] As one commentator observes, this means that GDPR "creates a burden that 'runs with' the data subject's information."[245] In a similar vein, Article 82 provides that "[w]here more than one controller or processor, or both a controller and a processor, are . . . responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage . . . ."[246] In other words, controllers cannot evade liability by asking a third-party to process a data subject's information. This resembles joint and several liability, a concept that is usually associated with tort law. But in this case, it enables data subjects to enforce their rights against third-parties.[247] Nor can processors escape by engaging sub-processors. The United Kingdom's ICO, which publishes interpretations of GDPR, makes clear that data controllers, processors, *and* sub-processors can all be liable to a data subject.[248]

3. GDPR Limits Data Subjects' Ability to Alienate their Rights

For the most part, the Regulation prevents data subjects from waiving their rights.

As the leading privacy casebook explains, "GDPR's fundamental protections cannot be overcome through individual consent or contract."[249] That is, data subjects "cannot choose to 'opt out' from core protections," including the rights to exclude, transfer, destroy, and use.[250]

244. *Id.* art. 17(2).

245. Victor, *supra* note 131, at 525.

246. GDPR, *supra* note 1, art. 82(4).

247. Likewise, when data processors go beyond their role by "determining the purposes and means of processing," the Regulation treats them as "a controller in respect of that processing." *Id.* art. 28(10).

248. *See* INFO. COMMR'S OFFICE, ICO GDPR GUIDANCE: CONTRACTS AND LIABILITIES BETWEEN CONTROLLERS AND PROCESSORS 14–15 (2018), http://perma.cc/67YL-SLQC.

249. SOLOVE & SCHWARTZ, *supra* note 201, at 1172.

250. *See id*.

This prohibition closely resembles Paul M. Schwartz's "hybrid inalienability" theory.[251] In this way, GDPR ensures that the *in rem* character of those rights cannot be eroded through contracts. Notice that hybrid inalienability is not an essential feature of property; rather, it is an addition necessary for property rights in personal data to be meaningful, given the problem of onward transfer.[252] Because the Regulation bestows a standard bundle of rights, treats those rights as *in rem*, and prevents data subjects from alienating those rights, it effectively extends property rights in personal data.

GDPR has already prompted other nations to treat personal data as property.[253] Indeed, experts explain that "something reasonably described as 'European standard' data privacy laws" have become the norm.[254] Because "data flows lightly and instantly across borders," data processors often rely on chains of transfers that connect many countries.[255] The European Union (E.U.) has harnessed this feature of personal data to export GDPR. By forbidding transfers of data to countries that fail to adopt similar regulatory regimes, the Regulation encourages other nations to adopt property-like systems.[256] Even U.S.-based consumers benefit from this approach. For example, Facebook offers Americans the same rights that GDPR guarantees for E.U. citizens.[257] So does Microsoft.[258] Indeed, more than 6 million of Microsoft's American customers exercised their data subject rights in the Regulation's first year.[259] As *The Economist* observes, "[a]ny American firm that serves European customers [has] no

251. *See supra* Part II.B.3; Schwartz, *supra* note 14, at 2094.

252. For a discussion of the relationship between property rights on alienability, *see supra* Part II.B.3 (rejecting the argument that property rights demand complete inalienability).

253. *See generally e.g.*, Jerome, *supra* note 2 (discussing the California Consumer Privacy Act and similar legislation in Brazil and India). Of course, this is not all that GDPR does. For some examples, *see supra* notes 210–212.

254. *See* Schwartz & Peifer, *supra* note 203, at 122.

255. *See* Anu Bradford, *The Brussels Effect*, 107 NW. U.L. REV. 1, 25 (2012).

256. *See* GDPR, *supra* note 1, art. 3(2) (explaining that GDPR applies to foreign processors offering goods and services to EU citizens, or who monitor the behavior of EU citizens in the EU).

257. *See* Josh Constine, *Zuckerburg Says Facebook Will Offer GDPR Privacy Controls Everywhere*, TECH CRUNCH (Apr. 4, 2018) (quoting Facebook CEO Mark Zuckerberg saying that, "[o]verall I think regulations like [GDPR] are very positive" and promising to "make all the same controls available everywhere, not just in Europe"), [http://perma.cc/DL3L-BWB5].

258. *See* Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

259. *See* Julie Brill, *GDPR's First Anniversary: A Year of Progress in Privacy Protection*, MICROSOFT (May 20, 2019), https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/.

choice but to comply with the GDPR; some firms plan to employ the rules world-wide."[260]

Thanks to GDPR, property rights in personal data are no longer a matter of theory. Instead, they have been adopted by the world's largest market, and are likely to spread to other markets as well.[261] This makes the question of how to secure those rights all the more urgent. After all, "property cannot exist without some institutional structure that stands ready to enforce it."[262] Drawing on examples from GDPR, the final Part of this Article shows that securing property rights in personal data may be less costly than previously thought.

IV. SECURING PROPERTY RIGHTS IN PERSONAL DATA

The second half of Demsetz's formula recognizes that the appeal of property rights turns on the cost of securing those rights.[263] As Thomas Merrill observes, "property cannot exist without some institutional structure that stands read to enforce it."[264] Under the traditional view, "th[at] institution is the state."[265]

Consistent with the conventional wisdom, most privacy scholars assume that governments have a monopoly on securing property rights in personal data.[266] Two decades ago, Kenneth Laudon proposed the construction of a government-operated "National Information Market" to property rights.[267] Soon after, Paul M. Schwartz argued that a combination of the Federal Trade Commission (FTC), a Data Protection Commission, and a court-enforced private right of action could together protect

260. *America Should Borrow from Europe's Data-Privacy Law*, THE ECONOMIST (Apr. 5, 2018), https://www.economist.com/news/leaders/21739961-gdprs-premise-consumers-should-be-charge-their-own-personal-data-right.

261. *See* Schwartz & Peifer, *supra* note 203, at 122.

262. Merrill, *supra* note 21, at 733.

263. *See* Demsetz, *supra* note 5, at 350.

264. *See* Merrill, *supra* note 21, at 733.

265. *Id*.

266. *See* Lauden, *supra* note 55, at 699–701 (discussing the three primary sources of privacy protection in the U.S.: common law, the Constitution, and federal and state legislation).

267. *Id.* at 705. Schwartz distinguishes his approach as "decentralized" compared with Laudon. *See* Schwartz, *supra* note 14, at 2111. Specifically, Schwartz suggests that multiple institutions (such as the FTC, state attorneys general, or class action litigation) should protect property rights. *Id.* at 2083 n.145. Arguably, any statute that offers data subjects a private right of action—as GDPR does—deputizes private enforcers. *See* GDPR, *supra* note 1, art. 82. After all, a private right of action enlists property owners to *detect* violations of their rights. But because data subjects have few advantages over the state at detecting violations, a private right of action may do little to reduce the cost of protecting property rights. Part IV.B.3 argues that the provisions that delegate enforcement to data *processors* have more to recommend them.

property rights in data.[268] Along the same lines, recent scholarship takes it as a given that only regulators[269] or courts[270] are available to protect property rights.[271] Ultimately, all of these proposals assume that the state bears the burden of securing property rights in personal data.

This Part challenges the conventional wisdom. Rather than rely solely on the state to protect property rights, policymakers should deputize private adjuncts to define and enforce those rights.[272] This strategy for securing property rights has many virtues:

First, this approach enlists effective problem solvers. Compared with governments, data processing firms are in the best position to craft technology solutions that reduce the cost of defining and enforcing property rights.[273]

Second, while personal data's unique attributes—the aggregation imperative and the ease of onward transfer—frustrate government enforcement, they frequently facilitate enforcement by private adjuncts. To take one example, the ease of onward transfer means that multiple data processors handle each piece of data, and thus are available to monitor one another's compliance with property rights.[274]

Finally, while property rights in personal data are new, the institutions that secure them need not be. In practice, traditional forms of property are protected by private adjuncts, not governments.[275] By using these

268. *See* Schwartz, *supra* note 14, at 2110–15.

269. *See, e.g.*, Hazel Grant & Hannah Crowther, *How Effective Are Fines at Enforcing Privacy?*, *in* ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 287 (David Wright & Paul De Hert eds. 2016) (arguing that "the vast fining powers in the new [GDPR] . . . suggest that in Europe at least both legislators and regulators believe that fines can have the desired effect").

270. *See e.g.*, Bergelson, *supra* note 14, at 450 (recommending "a private cause of action, legal fees . . . injunctive relief, and damages").

271. *See id.* Another recent work posits that property rights could be secured by "blockchain distributed ledger technologies." But the authors disclaim "[i]n-depth discussion" of how blockchain would enforce property as "beyond the scope of this paper." Ritter & Mayer, *supra* note 15, at 275–76.

272. *See, e.g.*, Williamson & Kerekes, *supra* note 26, at 564 (observing that "formal mechanisms may not be sufficient to achieve property rights institutions because of potentially high costs that are often understated or completely ignored"). Economists increasingly recognize the appeal of informal institutions that are not operated by the government. *See id.* at 558–64 (presenting results of empirical work that "suggests that informal institutions are the underlying channels that establish secure, well-defined property rights").

273. *See, e.g.*, Robert C. Ellickson, *Of Coase and Cattle: Dispute Resolution Among Neighbors in Shasta County*, 38 STAN. L. REV. 623, 686 (1986) ("Because it is costly to carry out legal research and to engage in legal proceedings, a rational actor often has good reason to apply informal norms, not law, to evaluate the propriety of human behavior.").

274. *See infra* Part IV.A.2.

275. *See* Claudia R. Williamson, *Securing Private Property: Formal versus Informal Institutions,* 54 J. Law & Econ. 537 (2011).

institutions as templates, policymakers can accelerate propertization. The bottom line is that deputizing private adjuncts may well secure property rights in personal data cheaply, quickly, and efficiently. Table 2, below, summarizes three reasons why this is so.

Table 2: Three Reasons for Optimism about the Feasibility of Securing Property Rights in Personal Data

	Conventional Wisdom	Reality	Prescription
1	Data processors are the problem.	Data processors are the solution because they are well-positioned to secure personal data.	Delegate key responsibilities (e.g., tracking data owners) to data processors.
2	The unique features of personal data frustrate efforts to secure property rights.	The unique features of personal data often facilitate efforts to secure property rights.	Construct institutions that harness personal data's unique features.
3	Personal data is different, so institutions that secure property rights must start from scratch.	Institutions that work in traditional property areas can also be useful here.	Rather than designing new institutions from scratch, begin with existing institutions as templates.

This Part proceeds as follows. Together, the first two Sections illustrate the virtues of mobilizing private adjuncts by presenting examples drawn from GDPR. Though this aspect of the Regulation has gone unrecognized, GDPR involves private parties in almost every aspect of securing property rights.[276] The first Section shows how GDPR enlists private adjuncts to define property rights. The second Section shows how GDPR deputizes private adjuncts to enforce those rights. The third and final

276. Outside of the context of personal data, some legal scholars recognize that private adjuncts help protect property. *See, e.g.*, John Rappaport, *Criminal Justice, Inc.* 118 COLUM. L. REV. 2251 (2018) (describing how private adjuncts help retailers secure property rights by adjudicating disputes and sanctioning shoplifters). Likewise, a growing economics literature acknowledges that both formal institutions ("government defined and enforced constraints") and informal institutions ("private constraints") can secure property rights. *See* Claudia R. Williamson, *Informal Institutions Rule: Institutional Arrangements and Economic Performance*, 139 PUB. CHOICE 371, 371 (2009).

Section addresses several nuances that complicate the case for mobilizing private enforcers.

A. Defining Property Rights

As Douglass North observes, "the creation of new property rights demands new institutional arrangements to define and specify the way by which economic units can co-operate and compete."[277] This Section introduces three institutions that define property rights in personal data.

1. Identifying the Property Owner

For property rights to be secure, prospective purchasers must be able to tell which bundles of rights belong to which owners. "Knowledge about title to property rights is crucial to enjoying their value," as one observer attests.[278] So it is no surprise that "every American state" has a public recording system to maintain land title records.[279] Under this system, anyone—whether a buyer, seller, or interested third-party—"can ascertain who owns land in the county by searching the records."[280] Public records serve multiple functions. For property owners, title increases certainty of ownership, "*facilitating* transactions in licit markets."[281] At the same time, recording systems also "hinder[] nonconsensual appropriations of property by illicit parties, such as thieves . . . ."[282] It is more difficult to sell stolen property when prospective purchasers can tell that it is stolen.

At first glance, adopting a title recording system for personal data seems counterproductive. After all, title records link an owner with a specific piece of land. But public registries that link data with a data subject would not protect personal data. Rather, those records would disseminate the data they aim to protect.[283] GDPR overcomes this obstacle by providing one way for data subjects to show title to their data, and another way for prospective purchasers to verify ownership.

277. NORTH & THOMAS, *supra* note 6, at 5.

278. *See* Abraham Bell & Gideon Parchomovsky, *Of Property and Information*, 116 COLUM. L. REV. 237, 241 (2016).

279. JESSE DUKEMINIER ET AL., PROPERTY 662 (9th ed. 2016).

280. *Id*.

281. *See* Bell & Parchomovsky, *supra* note 278, at 263.

282. *See id*. at 242.

283. *See id.* at 273–74. To some degree, this resembles the Heisenberg uncertainty principle: it is difficult to observe personal data without changing its value. *See* Katazyna Kloc et al., *Basic Compliance*, *in* Guide to the GDPR (Maceij Gawronski ed. 2019) (arguing that compliance with such a system would "be like the Schrödinger's Cat mixed with Heisenburg's uncertainty principle").

First, the Regulation provides data subjects with a way to prove title to their property by obliging data controllers to maintain ownership records.[284] Article 7 demands that controllers "be able to demonstrate that the data subject has consented to processing of his or her personal data."[285] To do this, controllers must retain a record that links the data subject's identity with proof of consent, often in the form of an e-signature or equivalent.[286] Further, Article 12 provides that "where the controller has reasonable doubts concerning the identity of the natural person making the [data subject request], the controller may request the provision of additional information necessary to confirm the identity of the subject."[287] This approach ensures that data subjects, the property owners in this scenario, can confirm ownership.[288]

Second, GDPR deploys a novel approach to avoid publicizing data ownership information. When a third-party needs to identify who owns a particular piece of personal data, the Regulation directs them to look at the data itself.[289] By nature, personal data identifies a person—otherwise, it is not personal data.[290] GDPR provides only one avenue for data controllers and processors to gain complete ownership of personal data: de-identification, sometimes referred to as anonymization.[291] So, a third-party reviewing the data can identify its owner by examining the structure of the data itself.[292] If the data can be associated with a person, then it belongs to *that* person. And, if it cannot be associated with a person, then the data belongs to whichever data controller or processor possesses the

284. *See* GDPR, *supra* note 1, art. 7.

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

286. *See How Should We Obtain, Record and Manage Consent?,* INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/ (last visited May 29, 2020).

287. GDPR, *supra* note 1, art. 12(6).

288. One concern is that this system encourages data processors to bombard data subjects with requests to verify their data. *See infra* Part IV.C.3 (discussing this and other costs of transitioning to a propertization regime).

289. *See* GDPR, *supra* note 1, art. 13.

290. *See id.* art. 4(1) ("'[P]ersonal data' means any information relating to an identified or identifiable natural person.").

291. *See id.*, art. 11(2) ("Where . . . the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply [except in certain limited circumstances].").

292. GDPR might improve by providing a bright-line rule for de-identification. For instance, the Health Insurance Portability and Accountability Act (HIPAA) provides a list of eighteen enumerated data elements. *See* 45 CFR § 164.514(b)(2) (2020). If the data controller removes all of these elements, the personal information is considered de-identified. *See id.* § 164.502(d). *See also* SOLOVE & SCHWARTZ, *supra* note 201, at 523.

information.[293] When the proper owner of data is ambiguous, the burden is on the data subject to demonstrate ownership.[294]

Together, these approaches improve on the public recording system by enlisting private adjuncts to identify data owners and maintain ownership records. This strategy does more than merely shift costs from a government records office to private parties. Indeed, while public registries are expensive and not always accurate, GDPR's approach promises to be relatively inexpensive for all parties.[295] For one, data controllers may be particularly well-positioned to identify data owners accurately and to store ownership information efficiently. For another, this strategy minimizes the cost to data subjects. Since data controllers maintain records, data subjects need not keep their own records or conduct complex analyses to identify their data. And because the owner's identity is inherent in personal information, data subjects do not need to do anything to mark information as their own. In short, GDPR turns one attribute of personal data into an advantage, inaugurating a decentralized, low-cost system for identifying owners.

2. Accounting for Complementarities

To protect property rights, it is often necessary to limit uses of neighboring property.[296] To see why, suppose that you own a home, but have no way of stopping a factory from moving in next door and filling your home with smoke. In that case, it would be difficult to describe your property rights as secure.[297] Protecting property requires institutions, such as zoning ordinances, that ensure that lots conform to certain sizes or be dedicated to particular purposes.[298]

293. As the success of the data broker industry attests, data controllers and processors should be able to secure this information through contract and trade secret law. *See supra* Part I.B.2.

294. *See* GDPR, *supra* note 1, art. 11(2) ("Where . . . the controller is able to demonstrate that it is not in a position to identify the data subject [the data subject rights] . . . shall not apply except where the data subject . . . provides additional information enabling his or her identification.").

295. *See generally e.g.*, Orr v. Byers, 244 Cal. Rptr. 13 (Cal. Ct. App. 1988) (detailing the consequences of "a misspelled name" in a title record). *See also* PONEMON INST. LLC, THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS: BENCHMARK STUDY OF MULTINATIONAL ORGANIZATIONS 3 (2017) (concluding that "if companies spent more on compliance activities . . . it would be less costly than if they were in non-compliance with data protection regulations").

296. *See, e.g.,* Vill. of Euclid v. Ambler Realty Co., 272 U.S. 365, 394 (1926) (explaining that limitations imposed by zoning have benefits for the property rights of residential owners).

297. *See id.* (discussing the benefits of having detached homes and apartment homes in adjacent areas).

298. *See, e.g.*, *id*. at 387–89 (describing the development of municipal zoning laws).

The need to manage adjacent property is not limited to land. Consider patent law.

In that context, private standard-setting organizations (SSOs) fill the same role as municipal zoning laws.[299] Like zoning boards, SSOs set standards for different technology "neighborhoods."[300] In this way, SSOs "allow[ ] compatibility between products made by different manufacturers."[301] As Mark Lemley observes, "[s]imply agreeing on a standard . . . has value . . . ."[302] Without limits on neighboring uses—or technology formats—property rights are precarious.

When it comes to personal data, constructing institutions that account for complementarities is critical. As discussed in Part I.A.1., much of the value of personal data depends on aggregation.[303] The more data structured in a particular format, the more data that can be combined, and the more valuable that data is. Conversely, as formats proliferate, it becomes more likely that data will be trapped in an isolated format.

To address this problem, GDPR directs data processors to identify industry-standard formats for personal data.[304] The Regulation requires processors to provide data subjects with information in a "structured, commonly used, and machine-readable format."[305] In practice, this means industry groups will need to coalesce around standard formats. For example, telecommunications providers could identify a standard format for storing cellphone location data. In addition, GDPR affords data subjects "the right to have [their] personal data transmitted directly from one controller to another, where technically feasible."[306] Accordingly, data processors must collectively define standard formats.[307] In this way, GDPR both permits and encourages data processors to identify standard formats. This approach looks more like an SSO than a local zoning board. Rather than mandating particular formatting requirements, the Regulation leaves

299. *See generally* Mark A. Lemley, *Intellectual Property Rights and Standard-Setting Organizations*, 90 CAL. L. REV. 1889 (2002) (describing the functions and justifications for SSOs).

300. *See id.* at 1892.

301. *Id*. at 1893.

302. *Id*. at 1897.

303. *See supra* Part I.A.1.

304. *See* GDPR, *supra* note 1, art. 13.

305. *Id.* art. 20(1). Note that this right does not apply to data that is not processed through automatic means, or in the limited cases when data is not processed according to consent or contract.

306. *Id.* art. 20(2).

307. For more details, *see generally Right to Data Portability*, INFO. COMMISSIONER'S OFF. (June 9, 2018, 11:33 PM), http://perma.cc/2G6L-RQBY (defining standard terms and formats for the right to data portability).

it to private parties with relevant technical knowledge to identify standards. This is particularly important when it comes to personal data, as the state of the art—and even the types of data being collected—evolves rapidly.[308]

The unique attributes of personal data make it easy for SSOs to enforce formatting standards.[309] Because of the need to aggregate information, data processors have an incentive to adhere to SSO-defined formats. After all, data that conforms to those formats will be more valuable than data that does not. Further, because of the prevalence of onward transfer, data processors will need to abide by standards to share information with others. For this reason, the standards set by SSOs are likely to be self-enforcing. In this way, personal data's unique attributes facilitate a relatively inexpensive institution to manage the complementarities associated with property.

3. Defining the Scope of Property

To secure property rights, it is necessary to define the scope of those rights. For traditional forms of property, the *numerus clausus* principle serves that function. Under that principle, property interests must "conform to a finite list of recognized forms."[310] Land, for example, can be held in a limited number of forms, such as "the fee simple, the defeasible fee simple, the life estate, and the lease."[311] The usefulness of this principle does not depend on the specific rights contained in each form. As the leading paper explains, "[l]imiting the number of basic property forms allows a market participant or a potential violator to limit his or her inquiry to whether the interest does or does not have the features of the forms on the menu."[312] In short, "limiting the number of forms . . . makes the determination of their nature less costly."[313]

GDPR embraces the *numerus clausus* principle. The Regulation starts with the presumption that data subjects own their data outright—similar to a fee simple.[314] At the same time, GDPR also grants data

308. *See, e.g.*, Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 435, 448–49 (2018) (describing new technologies that collect "biometric, health-related, and highly-sensitive data").

309. *See supra* Parts I.A.1 & I.A.2.

310. Thomas W. Merrill & Henry E. Smith, *Optimal Standardization and the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1, 9 (2000).

311. *Id*. at 3.

312. *Id*. at 33.

313. *Id*.

314. *See generally* GDPR, *supra* note 1, arts. 15–20 (granting data subject various rights, including the right of access, right to rectification, and right to erasure).

controllers the equivalent of fee simple ownership of any personal information that they de-identify.[315] Indeed, it provides that whenever a "controller is able to demonstrate that it is not in a position to identify the data subject . . . [the data subject rights in] Articles 15 to 20 shall not apply."[316] Alternatively, GDPR affords data subjects the right to alienate their data in a form that can be compared to a lease or a bailment.[317] Like a landlord, the data subject consents to transfer their property interest to a data controller for a defined time period.[318] During that time, the controller can use, enjoy, and even—in some circumstances—share the personal information with third-parties.[319] But, just as with a lease, certain uses are forbidden. For instance, the Regulation forecloses uses that are inconsistent with what it calls "compelling legitimate grounds" or the "legitimate interests" of the controller."[320] Should the controller exceed these limits, the data subject, as residual owner, can object and reclaim his or her full property interest.[321] Likewise, the data subject retains residual rights that resume when the "lease" expires—that is, whenever the original objective of the processing is complete.[322] Table 3, below, summarizes the limited menu of property rights available under GDPR.

315. *See id.* art. 11 (stating that the rights granted to the data subject in Articles 15–20 do not apply with respect to de-identified information).

316. *Id.* art. 11(2). Note that this Article allows data subjects to provide "additional information enabling his or her identification." *Id.* Articles 12, 13, and 14, which provide data subjects about notice about how their information is being used, still apply to de-identified data. *See id.*

317. *See infra* Table 3.

318. *See* GDPR, *supra* note 1, art. 7.

319. *See id*.

320. *Id.* art. 6. While GDPR does not elaborate on what qualifies as a legitimate interest, the UK ICO has explained that, "legitimate interests can be your own [that is, the controller's] interests or the interests of third parties. They can include commercial interests, individuals interests, or broader societal benefits." *Legitimate Interests*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (last visited May 29, 2020).

321. GDPR, *supra* note 1, art. 21.

322. *See id.* art. 5(1)(c) (introducing a "data minimization" principle that requires data processors to delete data when it is no longer necessary for the original purpose). For a discussion of the data subject rights, *see supra* Part III.B.

Table 3: GDPR's *Numerus Clausus*

Type of Interest	Data Subject's Interest	Data Controller's Interest	Description
Data Subject Owns	Fee Simple Absolute	No interest	GDPR presumes that data subjects have a fee simple interest in their data
Data Controller Owns	No interest	Fee Simple Absolute	GDPR permits data controllers to gain a fee simple in personal data if they anonymize it[323]
Data "Lease"	Remainder interest, ownership reverts when certain conditions are met	Leasehold interest subject to limitations	A full ownership interest returns to the data subject when the controller engages in impermissible processing or when the data no longer necessary for the original purpose

323. Another interpretation is that, since anonymous data is not personal data, it no longer qualifies as property at all. Regardless, the effect is the same: data processors can do whatever they want with the anonymized data in question.

Admittedly, GDPR's adoption of the *numerus clausus* principle relies more on the state, and less on private adjuncts, than the other institutions introduced here. Not only did legislators design this specific menu of interests, but regulators will police deviations from that menu—at least in the short term. But in the long term, the promise of the *numerus clausus* principle is that it may become an informal, universally-understood constraint that is enforced primarily through social sanctions.[324] As Robert Ellickson explains, "[b]y recognizing a standard [property] bundle, a group can simplify its members' interactions and transactions."[325] The more that data processors trade data that that is subject to GDPR's menu of rights, the more they will design systems that implement and enforce that menu. Over time, these informal norms may become so entrenched that state support becomes unnecessary.

Taken together, the institutions described here define property rights in personal data. By enlisting private adjuncts to identify owners, manage complementarities, and delineate the scope of property, these institutions define rights in personal data more cheaply, quickly, and efficiently than the state. Of course, the more clearly that property rights are defined, the easier it is to detect violations adjudicate disputes. The next Section introduces institutions that do just that.

B. Enforcing Property Rights

Thanks to the ease of onward transfer, enforcing property rights in personal data is a tall order.[326] To compensate, enforcement mechanisms must be as fast and cheap as possible. This Section demonstrates how enlisting private adjuncts can accelerate enforcement of property rights.

1. Resolving Disputes

Courts are not the only way to resolve disputes.[327] To the contrary, Robert Ellickson's famous study of Shasta County cattle ranchers identified four alternative types of dispute resolution: "self-help retaliation," "[informal] reports to [government] authorities," "claims for compensation informally submitted [to the tortfeasor] without the help of attorneys," and "formal legal claims."[328] In practice, ranchers resolve their differences through informal mechanisms far more often than through

324. *See, e.g.*, Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1362 (1993). In this case, those sanctions might include reputational damage or the threat of exit by customers and third-parties.

325. *Id*.

326. *See supra* Part I.A.2.

327. *See* Ellickson, *supra* note 275, at 677.

328. *Id*.

"formal legal claims."[329] As Ellickson explained, "it is costly to carry out legal research and to engage in legal proceedings, [so] a rational actor often has good reason to apply informal norms, not law. . . ."[330]

Private dispute resolution has as many advantages for data subjects and processors as it does for cattle ranchers. In many cases, private entities already have the technical capacity to evaluate property owners' claims efficiently.[331] So it is no surprise that GDPR repeatedly instructs data subjects to vindicate their rights by engaging directly with data processors.[332] At the same time, GDPR also provides courts and regulatory bodies to adjudicate grievances.[333] So it remains to be seen how often disputes will be resolved through private channels.

That said, early indications suggest that private dispute resolution will predominate. Consider the right to be forgotten.[334] That right was initially recognized in a 2014 court decision, *Google Spain*,[335] and later codified in GDPR.[336] Because the right to be forgotten has been in place since 2014, it provides a preview of how disputes may be resolved under GDPR.[337] Every year since the *Google Spain* decision, Google has published a Transparency Report that details its approach to evaluating claims based on the right to be forgotten.[338] Two lessons from that Report deserve attention.

First, private resolution of disputes about data subject rights is fast and cheap. Recall Demsetz's teaching that technology can significantly

329. *See id.*

330. *Id.* at 686.

331. *See, e.g.*, *infra* at 341–344.

332. *See* GDPR, *supra* note 1, art. 15(3) ("The controller shall provide a copy of the personal data undergoing processing."); *id.* art.16 ("The data subject shall have the right to obtain from the controller . . . the rectification of inaccurate personal data . . . ."); *id.* art. 17(1) ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her . . . ."). These key provisions direct data subjects to assert their rights by engaging with data processors, not with courts.

333. *See id.* art. 72 (permitting data subjects to bring claims in court); *id.* art.77 (permitting data subjects to lodge a complaint before data protection regulators).

334. *See* GDPR, *supra* note 1, art. 17.

335. *See* Court of Justice Press Release No. 70/14, Judgment in Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja Gonzalez (May 13, 2014).

336. *See* GDPR, *supra* note 1, art. 17. The "right to erasure," resembles the "right to be forgotten." *See Erasure of Online Information: European Union*, LIB. OF CONGRESS, https://www.loc.gov/law/help/erasure-online-info/eu.php (last visited May 29, 2020).

337. *See e.g.*, Court of Justice Press Release, *supra* note 340 (holding that individuals have the right to ask search engines like Google to delist certain results for queries on the basis of a person's name).

338. *See Transparency Report: Overview*, GOOGLE, http://perma.cc/4WTU-KBCR [hereinafter Google Transparency Report].

reduce the cost of enforcing property rights.[339] Compared with courts and regulators, data processors are—almost by definition—better equipped to develop technologies that can quickly and cheaply resolve disputes.[340] In this case, data subjects complete a simple web form accessible from their Google Account.[341] In stark contrast with complaints filed before regulatory authorities or courts, submitting a request only takes a few minutes to complete. Even critics of *Google Spain* acknowledge that it succeeded "in fashioning a . . . cheap and comprehensive" private enforcement system.[342]

Second, perhaps because they recognize the advantages of private dispute resolution, European regulators have largely left adjudication to Google and other search engines.[343] Every day, Google adjudicates several thousand content removal requests.[344] This represents the vast majority of right-to-be-forgotten complaints.[345] Yet regulators almost never intervene.[346]

Google's process for enforcing data subjects' right to be forgotten illustrates the benefits of private dispute resolution. Compared with adjudication by courts and administrative agencies, private dispute resolution offers lower costs and faster answers.[347] Indeed, private dispute resolution may be especially effective in the context of personal data. By definition, data processors analyze data at scale. So the resolution of one violation of data subject rights can be broadly applied almost instantly.

339. *See* Demsetz, *supra* note 5, at 350 ("[T]he emergence of new private or state-owned property rights will be in response to changes in technology and relative prices.").

340. *See* James D. Prendergast, *The Use of Data Processing in Litigation*, 17 JURIMETRICS J. 227, 237 (1977).

341. *See* Google Transparency Report, *supra* note 338.

342. Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, The Right to be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 1068 (2018). These critics worry about the impact of the right-to-be-forgotten on free speech. The extent to which property rights in personal information tread on free speech interests is an interesting question that deserves more attention, but is beyond the scope of this Article.

343. *See* Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017, 1035–36 (2016).

344. *See* Google Transparency Report, *supra* note 338 (noting there have been 931,612 requests to delist and 3,660,582 URLs requested to be delisted as of May 29, 2020). Note that the scope of the right to be forgotten under *Google Spain* is considerably narrower than under GDPR Article 17's right to erasure, which does not apply only to search engines. *See* GDPR, *supra* note 1, art. 17.

345. *See* Post, *supra* note 342, at 1067.

346. Google Transparency Report, *supra* note 338 (listing very few instances where European regulators reversed or even questioned Google's response to a content removal request).

347. *See* Todd B. Carver & Albert A. Vondra, *Alternative Dispute Resolution: Why It Doesn't Work and Why It Does*, HARV. BUS. REV. (May–June 1994), https://hbr.org/1994/05/alternative-dispute-resolution-why-it-doesnt-work-and-why-it-does.

To be clear, private adjudication requires some form of public adjudication as a backstop. After all, in the absence of state intervention, it is not obvious that controllers like Google would adjudicate data subjects' claims fairly. So, while private dispute resolution can shoulder part of the burden of adjudicating property rights, it cannot entirely replace courts and regulators. Still, following in the footsteps of Ellickson's ranchers, policymakers should specify property rights in ways that encourage private resolution of disputes as much as possible. GDPR does exactly that.

2. Deputizing Third-Party Enforcers

Who enforces property rights? When it comes to land, police officers and government regulators certainly play a role.[348] Property owners also contribute, either through self-help or by bringing complaints before courts and regulators.[349] Less obviously, property owners also count on third-parties to protect their rights.[350] As Thomas W. Merrill and Henry E. Smith explain, "much of the protection that property owners enjoy comes from a general respect for property rights and from the fact that third parties informally monitor and help to enforce such rights."[351] For example, neighbors can watch one another's land and take action—either alerting the owner or calling the police—if an outsider interferes. This monitoring does not replace a police force altogether, but it does reduce the need for government enforcers.

Unlike land, personal data is usually not visible to outsiders, so it may not seem susceptible to monitoring by third-parties. In keeping with that intuition, legal scholars have concentrated on how state-operated institutions—from regulatory agencies to class action litigation—can enforce individuals' rights in data.[352] But recall that personal information is normally shared with many third-party data processors.[353] Like next-door neighbors who watch one another's property, those data processors are well-equipped to monitor property rights in data. By definition, they understand how to process, store, and analyze data—and they have the

348. *See* Justice Philip A. Talmadge, *The Myth of Property Absolutism and Modern Government: The Interaction of Police Power and Property Rights*, 75 WASH. L. REV. 857, 857–58 (2000).

349. *See* Anna di Robilant, *Property: A Bundle of Sticks or a Tree?*, 66 VAND. L. REV. 869, 893–94 (2013).

350. *See* Merrill & Smith, *supra* note 91, at 796.

351. *Id.*

352. For an entire volume of articles that take this approach, *see* ENFORCING PRIVACY: REGULATORY, LEGAL, AND TECHNOLOGICAL APPROACHES (David Wright & Paul De Hert eds. 2016).

353. *See supra* Part I.B.2 (discussing how data brokers share the same datasets with many different partners).

further advantage of routinely interacting with the data set in question. So, just as neighbors reduce the need for a local police force, data processors reduce the need for costly government enforcers.

To take one example, Apple has emerged as "a kind of privacy regulator for the rest of the tech industry."[354] Because Apple controls "what code people can run on their own phones," it has the capacity to punish third-party firms who abuse privacy protections.[355] Recently, Facebook "violat[ed] Apple's rules with a research app that allowed Facebook to snoop on users' online activity."[356] In response, Apple "cut[ ] off Facebook's access to apps and updates that it was working on internally, causing chaos among the company's software engineers."[357] As this example illustrates, because data processing firms depend on one another's services, they have the ability to detect—and deter—missteps by other firms.

To secure property rights in data, the Regulation encourages firms to monitor one another.[358] Most important, GDPR treats controllers *and* processors as jointly "responsible for any damage caused by processing . . . ."[359] The Regulation explicitly instructs data controllers to monitor processors, stating that, "the controller shall implement appropriate technical and organi[z]ational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."[360] This may include certification, audits, and other forms of monitoring.[361] GDPR also directs processors to monitor any *sub*-processors they may use.[362] For instance, it commands that "[w]here that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."[363]

354. Kashmir Hill, *I Cut Apple Out of My Life. It Was Devastating*, GIZMODO (Feb. 5, 2019), https://gizmodo.com/i-cut-apple-out-of-my-life-it-was-devastating-1831063868.

355. *See id*.

356. Kevin Roose *Maybe Only Tim Cook Can Fix Facebook's Privacy Problem*, N.Y. TIMES (Jan. 30, 2019), https://www.nytimes.com/2019/01/30/technology/facebook-privacy-apple-tim-cook.html.

357. *Id*.

358. *See* GDPR, *supra* note 1, art. 82 (discussing the responsibilities of processors).

359. *Id.* art. 82(4) ("[E]ach controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject."). This is equivalent to the concept of joint and several liability in American tort law.

360. GDPR, *supra* note 1, art. 24(1); INFO. COMM'RS OFFICE, *supra* note 250, at 14–15.

361. *See id.* at 16.

362. *See* GDPR, *supra* note 1, art. 28(4); INFO. COMM'RS OFFICE, *supra* note 250, at 14–15.

363. GDPR, *supra* note 1, art. 28(4).

In this way, GDPR takes advantage of onward transfer, usually an obstacle to the enforcement of property rights.[364] The more that data processors exchange information, the more third-party monitoring will occur, reducing the need for intervention by regulators.[365] Likewise, when data processors deal with aggregated sets of data, enforcement that protects the property rights of one data subject is likely to protect the rights of many others. So, once again, the attributes of personal data make it easier, not more difficult, to protect property.

What do GDPR's requirements mean in practice? As *The Economist* observes, "[f]irms have to make sure that businesses from which they receive personal data, and ones to which they send such information, are also in compliance."[366] To avoid liability, every controller has an incentive to engage with processors that carefully protect data subjects' rights. Likewise, processors and sub-processors have a reason to avoid deals with controllers who fail to protect data subjects' property interests. By promoting shared liability, GDPR promotes "self-policing."[367] As with private dispute resolution, self-policing cannot entirely substitute for enforcement by regulators, but it can reduce the demand for that costly form of enforcement.

This Part has outlined five institutions that promise to secure property rights in personal data. Each institution enlists private adjuncts to define and enforce property rights. Each institution harnesses personal data's unique attributes to facilitate propertization. And each institution adapts traditional institutions, accelerating implementation. Together, these private adjunct-based institutions demonstrate that it is feasible to secure property rights in personal data. Table 4, below, summarizes these advantages.

364. *See supra* Part I.A.2 and Part I.B.2 (discussing how onward transfer enables data brokers to escape enforcement).

365. *See supra* Part IV.C.4 (addressing the objection that if data subjects cannot detect violations in the first place, then data processors have little incentive to enforce data subjects' rights).

366. *Europe's Tough New Data-Protection Law*, THE ECONOMIST (Apr. 5, 2018), https://www.economist.com/news/business/21739985-complying-will-be-hard-businesses-it-will-bring-benefits-too-europes-tough-new.

367. *See id*.

Table 4: Institutions that Secure Property Rights in Personal Data

A. Function	B. Property Law Analogue	C. Advantage of Deputizing Data Processors	D. How Personal Data Facilitates this Institution
Identify Property Owners	Land title records	Best situated to store and verify ownership information	The owner's identity is inherent in the structure of personal data
Account for Complementarities	Standard Setting Organizations (SSOs)	Best situated to identify appropriate format for data	The need to aggregate data makes standards mostly self-enforcing
Defining the Scope of Property	*Numerus clausus* principle	Best situated to design systems that apply a limited menu of property rights	The prevalence of onward transfer rewards data processors who enforce a standard menu of rights
Enforce Rights	Third-party enforcers	Best situated to monitor other data processors	Complex data flows encourage data processors to monitor one another
Resolve Disputes	Private dispute resolution	Best situated to detect violations, adjudicate disputes, and enforce results	Aggregation means that resolving one dispute also resolves many others

C. Complicating the Case for Private Adjunct-Based Institutions

Until now, this Part has identified the virtues of deputizing private adjuncts to secure property rights in personal data. At this point, however, it is important to acknowledge five nuances that complicate the argument. For the policymakers who design propertization regimes that follow GDPR's model, each complication offers guidance about to do—and what to avoid.

1. Private Adjuncts Require Continued Support from Regulators and Courts

Under GDPR, private parties determine data's rightful owners, set standard formats, adjudicate disputes, and enforce property rights.[368] But, even though private enforcers are the first line of defense, government regulators must stand ready as a backstop. This is an important difference between GDPR's regime and Robert Ellickson's cattle ranchers. Ellickson believed that ranchers' norms would be effective without the backstop of the formal legal system.[369] It is difficult to imagine the same would be true for personal data. This suggests that while GDPR can deputize private adjuncts, it cannot replace courts and regulators entirely.

But this is far from a fatal flaw. Though not a panacea, private adjuncts can shoulder much of the burden of securing property rights. Each of the five institutions presented above shows how private parties can help define and enforce property rights in personal data. And there is little doubt that data processors are likely to do a cheaper, quicker job than government regulators. The prescription for policymakers is clear. As more countries adopt propertization regimes,[370] policymakers should specify property rights in ways that maximize the involvement of private adjuncts, while recognizing the continued need for courts and regulators.

2. GDPR Puts the Fox in Charge of the Henhouse

Another concern is that GDPR gives data processors responsibilities that they may abuse. Once again, there is a critical difference between Ellickson's cattle ranchers and data processors. In terms of relative bargaining power, ranchers are typically on a roughly even playing field. That is not necessarily true of data subjects and data processing firms.[371] This may help explain why it is important to have government regulators as a backstop for private party enforcement and adjudication. In that case, if data processors refuse to protect property rights, data subjects can turn to the government for help. Even without government intervention, however, market forces may discourage abuse. Data processors who protect

368. *See* Michael Monajemi, *Privacy Regulation in the Age of Biometrics that Deal with a New World Order of Information,* 25 U. MIAMI INT'L & COMP. L. REV. 371, 377 (2018).

369. *See* Ellickson, *supra* note 275, at 685–86 (concluding that "the law of trespass had no apparent feedback effects on trespass norms").

370. *See supra* Part III (predicting that GDPR will spark propertization regimes in other countries).

371. Data processors, at least large technology companies like Google and Facebook, have market power. *See* Eric Posner & Glen Weyl, *The Real Villain Behind Our New Gilded Age*, N.Y. TIMES (May 1, 2018), https://www.nytimes.com/2018/05/01/opinion/monopoly-power-new-gilded-age.html.

personal data will gain the trust—and the high-quality data—of data subjects.[372] By contrast, data processors who shirk their responsibilities risk damaging their relationships with data subjects, and with the third-party data processors on whom they depend.

Of course, whether market forces limit abuse may depend on how competitive particular markets actually are. Some commentators fear that GDPR may reduce competition because the regulatory compliance burden is more easily borne by large firms.[373] That could lead to a vicious cycle, where legislation to protect property rights reduces competition, thus making it even more difficult to enforce those rights. Indeed, market concentration would also reduce the amount of third-party monitoring by other data processors.[374] Whether this troubling scenario will come to pass awaits further research, especially empirical analysis of how GDPR affects competition and market concentration.

3. Transition Costs Must be Taken into Account

This Part has examined the institutional costs of securing property rights. But it has had little to say about the costs of transitioning to that system. Given that the status quo does not include property rights, switching to a new regime imposes costs on data subjects, data processors, and regulators. Data subjects must learn about their newfound rights. Data processors must design technical systems that permit data subjects to monitor and enforce those rights. And regulators must promulgate guidance to help data processors understand the new regime.

Three factors suggest that the costs of transitioning to a property rights regime may be less substantial than first appears. First, transition costs are one-off, not ongoing, so they may not be significant in the long run—assuming that the propertization regime endures. Second, when it comes to GDPR, the most visible transition cost has been the barrage of notification emails that data processors have sent to data subjects.[375] Those communications derive from the Regulation's complex consent

372. *See supra* Part II.A.3 (discussing the topic of trust).

373. *See generally* Aysem Diker Vanberg & Mehmet Bilal Ünver, *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?*, 8 EUR. J.L. & TECH. 1 (2017) (arguing that lessons drawn from EU competition law may be used to limit the potential adverse consequences of the right to data portability).

374. *See supra* Part IV.B.2 (discussing the role that third-parties play in advancing property rights, and comparing it to personal data).

375. *See, e.g.*, Alex Hern, *Most GDPR Emails Unnecessary and Some Illegal, Say Experts*, THE GUARDIAN (May 21, 2018, 12:21 PM), http://perma.cc/TU52-KSD9 (explaining that GDPR does not require many of these opt-in consent requests).

requirements, not its creation of property rights in data.[376] Finally, GDPR's habit of adapting institutions from other areas of property, such as SSOs or the *numerus clausus* principle, reduces transition costs. It may easier for consumers and firms to understand the new system when it resembles familiar institutions from other areas of property.

4. GDPR Has Not Solved the Detection Problem

Still another objection is that obstacles to enforcement will persist.[377] Under both GDPR and the status quo, it is difficult for enforcers to detect violations of property rights.[378] After all, data processors use, store, and share data behind closed doors.

What this objection misses is that the creation of property rights in personal data provides new ways for data subjects to detect abuse. For instance, the right to access data requires processors to share the data that they have, and to explain how it is being used.[379] While data processors could misrepresent their data holdings or refuse to comply, those efforts to evade detection would themselves trigger liability. Further, the third-party enforcement mechanisms introduced above encourage data processors to scrutinize one another's activities for compliance.[380] In effect, this means that data processors—the parties who are best positioned to detect technological violations—have an incentive to do so. Even if some third-party data processors decide that detection is unlikely, the risk of a large fine may be enough to encourage remedial action by other processors with a lower risk tolerance.[381] The more variance in data processors' size and objectives, the better. For example, Google or Facebook may encourage third-party data processors to remedy violations—even when the risk of detection is low—rather than face large fines and reputational damage. This is not to say that GDPR will result in the detection of *every* property violation—only that these mechanisms should install powerful incentives to identify and remedy violations.

376. *See* GDPR, *supra* note 1, art. 7 (detailing the conditions for consent); *id.,* at Recital 32 (requiring "freely given, specific, informed, and unambiguous" consent). *See also supra* Part III.A (discussing the objectives of GDPR).

377. *See* Ritter & Mayer, *supra* note 15, at 226 (discussing enforcement conflicts and GDPR's view of data ownership).

378. *See id.* at 252.

379. *See* GDPR, *supra* note 1, art. 15(1)(a) (requiring controllers to disclose the purpose of data use); *id.* art. 15(3) (requiring controllers to provide "a copy of the personal data undergoing processing").

380. *See supra* Part IV.B.2 (discussing that the more data processors exchange information, the more third-party monitoring will occur).

381. *See* GDPR, *supra* note 1, art. 83(6) (providing for fines of up to 4% of total worldwide annual turnover for violations of data subject rights).

5. Privacy Protections Sometimes Undermine Efforts to Secure Property Rights

While this Part has used GDPR as a model of how to secure property rights, the Regulation also provides examples of what not to do. As Part III explained, GDPR pursues many objectives.[382] While many provisions work to secure property rights, others can be interpreted as undermining that objective. To take one example, GDPR permits data subjects to demand that any decision that significantly affects their legal rights be made by a person—not a machine.[383] This right, designed to advance privacy, may prevent data controllers from automating decisions that enforce data subjects' rights, increasing the cost of securing property rights.[384] As this example attests, privacy protections sometimes conflict with propertization. Policymakers should avoid promulgating requirements that frustrate efforts to deputize private parties to protect those rights.

Thanks to its emphasis on private adjuncts, GDPR does a surprisingly good job of securing property rights.[385] But there is room for improvement. Indeed, the nuances discussed here point towards a set of prescriptions for policymakers. First, policymakers should recognize that because some privacy protections undermine property rights, careful balancing of tradeoffs may be necessary. Second, more research is required to understand the relationship between propertization and competition. Finally, property rights impose transition costs on private parties that may be difficult to quantify. When designing new propertization regimes, policymakers must account for and minimize these costs. Above all, GDPR is only the first experiment in securing property rights in personal information. Now that the Regulation has gone into effect, empirical research can begin to evaluate the cost, speed, and effectiveness of the institutions introduced here. Undoubtedly, many refinements will be necessary.

CONCLUSION

This Article started with a simple question: has the time come to grant property rights in personal data? Demsetz's formula suggests that the answer is yes. The status quo is plagued by prohibitively high information costs and inadequate enforcement. Propertization promises to

382. *See* Part III.A (discussing the objectives of GDPR).

383. *See* GDPR, art. 22(1), *supra* note 1.

384. *See* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1017 (2017).

385. *See* Vlad A. Hertza, *supra* note 16, at 1731–1732 ("[The right to data portability] is one of the clearest indications that GDPR recognizes an interest akin to a person's property right in her or his personal data.").

mitigate—though not completely resolve—those challenges. Consistent with the growing appeal of propertization, the EU recently adopted a regulatory regime that effectively installs property rights in personal data: GDPR.

But for property rights to be secure in practice—not just desirable in theory—institutional investments are necessary. The conventional wisdom holds that the state, in the form of institutions like courts and regulators, has a monopoly on protecting property. GDPR illustrates a superior strategy. Rather than rely solely on the state to protect property rights, policymakers should deputize private adjuncts to define and enforce those rights. As a result, the case for extending property rights in personal data is stronger than previously thought.