CONTRACTING FOR PERSONAL DATA

KEVIN E. DAVIS† AND FLORENCIA MAROTTA-WURGLER‡

Is contracting for the collection, use, and transfer of data like contracting for the sale of a horse or a car or licensing a piece of software? Many are concerned that conventional principles of contract law are inadequate when some consumers may not know or misperceive the full consequences of their transactions. Such concerns have led to proposals for reform that deviate significantly from general rules of contract law. However, the merits of these proposals rest in part on testable empirical claims. We explore some of these claims using a hand-collected data set of privacy policies that dictate the terms of the collection, use, transfer, and security of personal data. We explore the extent to which those terms differ across markets before and after the adoption of the General Data Protection Regulation (GDPR). We find that compliance with the GDPR varies across markets in intuitive ways, indicating that firms take advantage of the flexibility offered by a contractual approach even when they must also comply with mandatory rules. We also compare terms offered to more and less sophisticated subjects to see whether firms may exploit information barriers by offering less favorable terms to more vulnerable subjects.

† Beller Family Professor of Business Law, New York University School of Law. B.A. McGill University; L.L.B. University of Toronto; L.L.M. Columbia Law School.

‡ Professor, New York University School of Law. B.A. University of Pennsylvania; J.D. New York University School of Law. We are grateful to Omri Ben-Shahar, Richard Brooks, David Hoffman, Paul Schwartz, Lauren Scholz, and Boris Segalis for helpful comments on an earlier draft as well as to participants in presentations at the U. of Pennsylvania Empirical Contracts Workshop, K-CON XIV, the 8th Annual Law and the Economics Conference in Consumer Law, the 9th Law and Economics Conference at the University of Lucerne, NYU Law Faculty Workshop, and Privacy Law Scholars Conference in Berkeley. We are also grateful for the support of the Filomen D'Agostino and Max E. Greenberg Research Fund at NYU School of Law. Ziv Ben-Shahar's assistance with the collection and coding of data was invaluable. Courtney Kan also provided excellent research assistance.

INTRODUCTION

If 'data is the new oil,' should markets for data be governed by the same rules as markets for oil?[1] In particular, should the ordinary principles of contract law apply? Is contracting for the collection, use, and transfer of data like contracting for the sale of a horse or a car or a piece of software?

Existing literature on these questions has focused on markets for personal data.[2] The protection of consumer information in the United States has followed a "Notice and Choice" approach, where businesses outline their information privacy practices, including representations, rights, and risk allocations in privacy policies, which are typically incorporated by reference in general Terms of Service contracts, to which users must agree.[3] To a large extent, the relationship between the business and user with regards to information privacy is contractual.

There is widespread concern that conventional principles of contract law are inadequate to protect the interests of consumers, who

---

[1] For a discussion and critique of the big data as oil analogy, see generally Lauren Henry Scholz, *Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies* (Fla. State Univ. Coll. of Law, Pub. Law Research Paper No. 895, 2018), https://ssrn.com/abstract=325254.

[2] *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004) (describing the emerging commodification of personal data); Sarah Spiekermann et al., *The Challenges of Personal Data Markets and Privacy*, 25 ELECTRONIC MKTS. 161 (2015) (summarizing economic, social, and political risks associated with markets for personal data).

[3] *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf ("Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."); *see also* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, at v (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("The Commission staff believes that consumer choice continues to play an important role.").

ostensibly agree to having their personal data collected by firms. A major fear, common in most transactions involving standard form contracts, is that consumers face barriers to information that lead them to misperceive or not fully internalize the nature and consequences of transactions.[4] The potential adverse consequences are significant. To begin, entities that collect and process personal data might use it in ways that are contrary to the true wishes or interests of consumers. For example, users of the pregnancy tracking app Ovia, who used it to record intimate details about their sexual lives, ovulation cycles, medications, pregnancy, as well as details of their lives with their newborns post-pregnancy, did not know that some of their employers had paid the firm, Ovia Health, to gain access to such information.[5] Or, as exposed by a number of data security breaches across various industries, collectors or processors might implement weak security measures that unduly increase the risk of unwanted release of personal and sensitive information.[6] Alternatively, the original collectors or processors might transfer the data to third parties who use or disseminate it improperly or who take inadequate or weaker than desired security measures. The ordinary remedies for breach of contract may be inadequate to deter or compensate for the particular harms caused by undesired or unauthorized use or dissemination of data.[7] And since

[4] *See, e.g.*, Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509 (2015) (surveying literature on people's uncertainty about the consequences of privacy-related behaviors and their own preferences over those consequences); Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 130–52 (discussing factors that prevent consumers from accurately estimating the increments in expected harm associated with data collection); *see also* OREN BAR-GILL, SEDUCTION BY CONTRACT: LAW, ECONOMICS AND PSYCHOLOGY IN CONSUMER MARKETS 2–3 (2012) (explaining how standard form contracts might include features designed to exploit consumers' misperceptions).

[5] While the firm shared information with employers and health insurers in an aggregate form, aggregate data on the percentage of high risk pregnancies of employees or how many dates of maternity leave were planned to be taken could affect the types of benefits offered, among other concerns. *See* Drew Harnwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST, (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think. Ovia's privacy policy also notes that users' identifiable information would be shared with employers or insurers when users "voluntarily" sign up for the app through their employer or insurer. *Ovia Health Privacy Policy*, OVIAHEALTH, https://www.ovuline.com/dynamic-privacy (last updated May 15, 2019).

[6] *See, e.g.*, IDENTITY THEFT RES. CTR., DATA BREACH REPORTS (2015), https://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf (describing the data security breaches of firms in various markets including Amazon, Aon Hewitt, Comcast, Home Depot, Target, T-Mobile, Sony, Hilton Worldwide, Uber, Trump Hotels, Costco, State Farm, American Airlines, and United Airlines).

[7] *See, e.g.*, *infra* notes 65–66 and accompanying text (explaining the potential inadequacy of expectation damages in deterring data breaches).

contractual rights and duties typically bind only the parties to the contract, they may be of limited value when data are transferred to other parties, a common practice in this environment.[8] While some of these problems are likely to affect both sophisticated parties (such as larger firms contracting for cloud computing services) and consumers alike, others are more likely to affect unsophisticated consumers who face information barriers as a result of their failure to read or understand information privacy related terms, or due to the aforementioned misperceptions.

These concerns have prompted proposals for reform that depart from fundamental principles and rules of contract law that govern other types of market transactions. Some of these reform proposals, which are the focus of our paper, would impose mandatory rules that cannot be amended by the parties to an agreement.[9] Those interventions, while addressing some of the problems outlined above, would also sacrifice the flexibility that is one of the key advantages of contractual governance. In the absence of mandatory rules, contracts can

---

[8] *See infra* note 61 and accompanying text.

[9] *See, e.g.*, PRINCIPLES OF THE LAW: DATA PRIVACY § 2 cmt. g (AM. LAW INST., Tentative Draft No. 3, 2018) (proposing principles that cover both data collectors and processors, compared to rules that primarily regulate data controllers and rely on voluntary contracting between controllers and processors to protect rights and responsibilities); Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1254–55 (2001) (arguing for more mandatory rules in the context of financial information privacy); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1675 (1999) (proposing a set of mandatory rules to control the extent of collection and use of personal data by commercial firms). For previous use by privacy scholars of the concept of default and mandatory rules, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246–65 (1998); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2404 (1996); Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 54–55 (1997). For general discussion of default and mandatory rules in the context of cyberspace, see Oren Bar-Gill & Omri Ben-Shahar, *Optimal Defaults in Consumer Markets*, 45 J. LEGAL STUD. S137 (2016), which examines optimal default rules in contexts where consumers are likely to be biased and uninformed about their own preferences regarding such default rules, such as the information privacy context; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1209–10 (1998); Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 745, which states that "[w]here private bargaining about data processing is unlikely to be successful, mandatory rules should set immutable standards to prevent failure in negotiations from producing social harm." Other proposals focus on choice architecture, such as creating opt-in defaults, which can be subsumed within the contractual paradigm to the extent that they preserve choice. *See, e.g.*, Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 1–10 (reviewing the notion of "notice and consent" regimes); Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61, 67 (2014) (noting the limitations of choice architecture in the privacy context).

be adapted to match the circumstances and needs of the parties, including as they change over time. By contrast, mandatory terms tend to be uniform and inflexible.

It is important to evaluate the empirical foundations for proposals seeking to address problems that result from information barriers that make consumers more vulnerable relative to more sophisticated parties. Proposals for special rules to govern the collection, use, security, and transfers of personal data rest at least in part on testable empirical claims whose careful evaluation should take precedence over anecdote and casual observation.

In this paper we suggest that by measuring the prevalence of privacy-protective contract terms across and within markets, as well as their evolution over time, we can provide a foundation for future research exploring the strength of these proposals. To this end, we examine 194 privacy policies from firms interacting with consumers in the United States across seven markets from 2014 to 2018 from a representative sample of firms. This is a subset of the firms that one of us (Marotta-Wurgler) examined in a previous study and includes all companies that remained in existence throughout the sample period and for which we could obtain privacy policies.[10] Ninety percent of the policies are incorporated by reference in the firms' "Terms of Use," where firms set out other contractual terms, including dispute resolution clauses. We analyze the terms that relate to collection, security, sharing of personal information, and enforcement of contractual rights and benchmark them against the 2012 self-regulatory guidelines of the Federal Trade Commission (FTC)[11] and the European Union's 2018 General Data Protection Regulation (GDPR).[12] We analyze the characteristics and changes of twenty-eight terms across ten categories, as articulated in the aforementioned guidelines, including commitments to ensure data accuracy, data retention practices, notice, privacy by design, contracts with processors of data, security measures, sharing practices, and user control, among others.

We warm up with a finding from Marotta-Wurgler's previous empirical work, which documented significant differences in informa-

[10] Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J. Legal Stud. S13 (2016).

[11] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[12] Regulation 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter GDPR].

tion privacy practices across markets.[13] Firms in markets that collect highly sensitive information (like adult entertainment firms) or where the subjects are likely to include more sophisticated users (like cloud computing firms) took more privacy protective steps in collecting, sharing, and securing personal data.[14] These differences offer evidence of the potential advantages of the flexibility associated with a traditional contractual approach in that they may reflect differences in preferences across markets. Subjects might want more protection in highly sensitive or potentially embarrassing situations, but require less for other uses of data, such as sharing on message boards. Permitting subjects to contract freely gives them the flexibility to enter into transactions that fit their varying needs.

Nonetheless, differences in information privacy practices across markets alone do not necessarily address the concerns guiding proponents of regulation. In particular, the terms in the policies might be exploitative in some dimensions or fail to fully internalize the contracting parties' preferences. We provide further evidence regarding the validity of these concerns by examining changes in information privacy practices over time and across parties and markets with varying levels of access to information.

The first step in our analysis is to isolate the effect of the GDPR, a significant revision of previous law on data protection and privacy for individuals within the EU that also governs the export of personal data outside the EU and applies to many U.S. firms. The GDPR became effective on May 25, 2018. It mandates information privacy practices and disclosures and imposes fines of up to four percent of annual global revenues on firms that violate its rules. The adoption of the GDPR during the sample period allows us to compare firms' reactions to a regulatory regime that imposes financial consequences for failure to comply (the GDPR) to one which relies mostly on self-regulation (the FTC's "Notice and Choice" approach).

We find that the vast majority of firms in the sample amended their terms right around the time when the GDPR became operational.[15] We also find that those terms that are regulated by the GDPR showed statistically significant improvements, on average, during the four-year period, in that they became more information-protective.[16] In contrast, those terms that were not subject to the

[13] *See* Marotta-Wurgler, *supra* note 10 (comparing the effect of third-party privacy standards and competitive forces in promoting the adoption of privacy protective terms in privacy policies and noting the variance across markets).

[14] *See id.* at S31–33.

[15] *See infra* Section III.A.

[16] *See infra* Section III.B.

GDPR became less protective, according to the relevant benchmarks, in a statistically significant way. While this shift may be a sign of concern, suggesting that firms are weakening protections for practices where they are afforded more flexibility, it may also reflect crowding out by the GDPR. For example, firms are now less likely to direct consumers to the FTC in case of information privacy complaints but also more likely to comply with various GDPR-dictated practices informing consumers about their rights. This is troublesome, however, as these are contracts directed to U.S. consumers.

More generally, we find that there are marked differences in contracting practices across markets that persist over time even after the GDPR.[17] We also find that compliance with the GDPR varies across markets in similarly intuitive ways, suggesting that firms take advantage of the flexibility offered by a contractual approach even when they must presumably comply with mandatory rules.[18]

We focus on the information privacy terms of cloud computing firms' privacy policies to examine whether firms are treating ordinary consumers differently from more sophisticated customers such as professionals or large firms. While we cannot draw any normative conclusions without more information about contracting costs and preferences, we find that, within markets, firms are not offering terms that could be seen as being maximally exploitative. We also find no significant differences between the terms offered to more and less sophisticated subjects within the cloud computing market. While these findings cannot lead us to draw firm conclusions about whether consumers will receive adequate protection from traditional principles of contract law that place few mandatory restrictions on contracting practices, they do invite further empirical analysis to determine whether traditional contract law is up to the challenge of governing transactions in personal data. In particular, future research should focus on assessing the extent to which firms' information privacy practices across markets line up with consumer privacy preferences and willingness to pay.

The Article proceeds as follows: Part I explains the mechanics of markets for data and outlines the potential benefits and pitfalls. Part II explores the role of contract in exchanges related to data transfer and security, provides an overview of the competing theories for data transfer governance, and offers an overview of existing governing regimes. Section III.A presents the data and methodology. Sections III.B, III.C, III.D, and III.E discuss the findings.

---

[17] *See infra* Section III.D.

[18] *See infra* Section III.D.

I
MARKETS FOR DATA

A. Examples of Markets for Data

A market is a group of actors collectively involved in production, exchange, and consumption of particular commodities. Markets can be defined and distinguished in terms of the types of commodities being exchanged, the identities of the participants, or their geographic locations.[19] Thus, we can speak of markets for food, clothes, music, narcotics, or sex, and market participants such as farmers, wholesalers, retailers, consumers, audiences, or performers. Some markets are extremely local, while others span the globe.

The subject of this Article is markets for data, and, in particular, data about identified or identifiable people (personal data).[20] The key participants are collectors and users of data. In some cases, the data being produced or exchanged are—or purport to be—about the attributes or behavior of specific subjects. Subjects may or may not have consented to or actively facilitated or even been aware of the collection of the data. Collectors and users sometimes interact through intermediaries, often known as brokers.[21] Still other actors assist in processing, storage, and communication of data.

To illustrate how some of these markets work, consider an hour in the life of a modern woman named Mia. After conducting one last search of an online legal database, she logs off from her employer's computer system. She uses her own device to check the weather and then, seeing rain in the forecast, uses it to hail a car for the ride home. During the ride, she browses the Internet. First, she checks the latest news about politics and the financial markets. Next, she turns to shopping for groceries, but this soon devolves into looking at clothes and videos or pictures of celebrities. She then logs on to a social network and views more of the same type of material. Sometimes she posts comments about what she sees, or simply "likes" it and reposts it to some or all of the people in her network. While she does this, she is

---

[19] *See, e.g.*, *Markets*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/mergers/markets (last visited May 27, 2019) (explaining the definition of a market in the context of mergers).

[20] This definition of personal data tracks the concept of Personally Identifiable Information 2.0 proposed by Paul M. Schwartz and Daniel J. Solove. 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, 1817 (2011).

[21] *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 3 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (describing the practices of data brokers and the privacy concerns raised by these practices).

listening to music streaming from an online provider. When she arrives at home, she uses a voice-activated smart speaker to purchase some of the food and clothes she viewed during her trip.

Over the course of an hour, Mia has actively participated in several data markets, in at least two different roles. As a user, she has consumed data about legal developments, weather, financial markets, and other news. She has also used traffic data through her ride-hailing app. At the same time, Mia also has been a prolific supplier of data. Her ride-hailing app almost certainly collected real-time data on her location. The apps she used to access her social network and to stream music most likely logged everything she saw, heard, and shared. The websites she visited would have collected data on her browsing activity and may have installed cookies on her browser. (Cookies are short pieces of code that collect information from a user's browser that can be accessed whenever the browser interacts with one of the maker's webpages.) More surprisingly to Mia, her Internet Service Provider might have collected her entire browsing history. There is also data about information that she has actively shared with some of these firms, such as her name, address, and credit card information, as well as any comments she has posted. Most of this data will pass through the hands of one or more intermediaries as it travels to its ultimate users, such as purchasers of advertising slots or websites and apps.[22]

B. Economic Effects of the Market for Data

One of the principal attractions of markets is that they enable mutually beneficial exchanges, in other words, exchanges of goods or services that render, or at least are expected to render, at least one party better off and neither party worse off.[23]

A necessary, but not sufficient, condition for a mutually beneficial transaction is that the transferee benefits from acquiring the data in question. There are several reasons why transferees might value data, but the most economically significant reason is that it helps them to make better decisions about how to act. Actions that might be

[22] José Estrada-Jiménez, Javier Parra-Arnau, Ana Rodríguez-Hoyos & Jordi Forné, *Online Advertising: Analysis of Privacy Threats and Protection Approaches*, 100 COMPUTER COMM. 32, 33–34, 37 (2017); *see also* FED. TRADE COMM'N, *supra* note 21 (reporting on the practices of intermediary data brokers who collect user data); David Nield, *Here's All the Data Collected from You as You Browse the Web*, GIZMODO (Dec. 6, 2017, 11:30 AM), https://fieldguide.gizmodo.com/heres-all-the-data-collected-from-you-as-you-browse-the-1820779304.

[23] *See* Benjamin E. Hermalin, Avery W. Katz & Richard Craswell, *Contract Law*, *in* HANDBOOK OF LAW & ECONOMICS 3, 21–23 (A. Mitchell Polinsky & Steven Shevell eds., 2007).

optimal in one state of affairs might be sub-optimal in another. Walking home might be optimal in sunny weather but not in the rain. A new steakhouse in Mia's neighborhood will find it worthwhile to send her its glossy brochure if she is a fan of the Paleo diet, but not if she is an observant Hindu. Drivers with access to real-time traffic data can plan their routes to minimize congestion. Researchers with access to medical data from a large population can identify harmful drug interactions and direct pharmacists to change their prescriptions accordingly.

In order for a transfer of data to be mutually beneficial, it would ideally benefit the transferor (oftentimes consumers seeking goods or services from firms) as well as the transferee. The impact of the transaction on the transferor will depend on both how much value the transferor receives in exchange for the data and the costs the transferor must incur. There are at least two reasons to believe that the transferor's costs will be low. First, in many contexts, consumption of data is nonrivalrous—the transferee's consumption of data does not interfere with the value that the transferor derives from it.[24] Second, the costs of effecting the transfer are likely to be extremely low since recent technological advances have dramatically diminished the costs of transmitting and storing data.[25]

Nonetheless, there are many reasons why it might be costly for the transferor to surrender data. When the transferor is the subject of the data, she may be concerned that the data will be used to expose her to: legal liability, as in the case of identity theft; discrimination; unwanted solicitations; social opprobrium; or the discomfort of being subject to surveillance. Mia might reasonably fear that an afternoon of data transactions will expose her to unauthorized credit card charges, higher prices at her favorite online stores, ads for trips to Croatia that follow her around the Internet, or stalkers. In other cases, where the transferor is a user rather than the subject of the data, the transferor may fear that disclosure will cause it to lose a competitive advantage. For example, Mia's favorite store might worry that its rivals will take

---

[24] *See* Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data* 1 (Stanford Graduate Sch. of Bus., Working Paper No. 3716, 2018) (contrasting data with rivalrous goods such as food or time that are depleted with use).

[25] *See* Lucas Mearian, *CW@50: Data Storage Goes from $1M to 2 Cents per Gigabyte*, COMPUTERWORLD (Apr. 10, 2017, 1:04 PM), http://images.techhive.com/assets/2017/04/10/cw-50th-anniversary-storage-trends.pdf (documenting the decrease in the cost of data storage); *How Much Does Data Really Cost an ISP?*, BROADBANDNOW (June 23, 2016), https://broadbandnow.com/report/much-data-really-cost-isps (noting that the cost of data transfers has historically trended downward, despite the rising cost of U.S. Internet connections).

advantage of a data breach to use targeted discounts to poach its customers.

Sometimes a mutually beneficial transfer of data is only possible if the transferee will abide by certain restrictions on the use or further transfer of the data or will implement security measures that reduce the risk of unintentional dissemination. For example, the transferee may agree not to use the data for purposes beyond those associated with completing the transaction or providing the service in question, or not transfer the data to anyone other than an affiliate or, in the case of a broker, a single client. The transferee also may agree to use the data only for the purposes of targeting certain types of advertising—e.g., direct mail as opposed to Internet advertising. Or the transferee may forgo certain types of advertising, such as political ads.

Some of these restrictions and security measures serve to limit the costs that data collection imposes on transferors who are consumers. For example, consumers might value the opportunity to provide anonymized medical data for research purposes, but be averse to allowing deanonymized versions of the data to be disseminated more widely and used to discriminate against or stigmatize them. Consumers might also fear unknown future uses of such data and how these may impact their lives. Other restrictions enhance the gains from trade by allowing the transferor to maintain and benefit from its market power in relation to the data. This is the case with restrictions which prevent the transferee from reselling the data in competition with the transferor. In addition, restrictions on use, in combination with restrictions on transfer, can help the transferor to charge different prices to different users—in other words, to price discriminate. Finally, restrictions on use may be designed to help avoid costly regulation. In the United States, for example, federal law regulates the collection and use of data for the purposes of determining access to credit, insurance, or employment.[26]

The benefits and costs of data transfers do not only accrue to the transferor and the transferee. For instance, society clearly benefits if the transferee will use the data to generate innovations that will be widely disseminated at relatively low charge. Transfers of data to medical researchers are prime examples of transactions that are likely to generate these kinds of spillover benefits.[27]

---

[26] Fair Credit Reporting Act, 15 U.S.C. § 1681(a)(d)(1) (2012).

[27] *See, e.g.*, Cynthia McFadden, Aliza Nadi & Rich Schapiro, *DNA Test Company 23andMe Now Fueling Medical Research*, NBC NEWS (Jan. 17, 2019, 8:10 AM), https://www.nbcnews.com/health/health-news/dna-test-company-23andme-now-fueling-medical-research-n958651.

Data transfers also generate spillover benefits when they serve to limit the market power of firms with privileged access to data. For example, a large bookseller like Amazon has direct access to vast amounts of consumer data which it can use to tailor new product recommendations to its customers' interests.[28] Smaller booksellers will be at a significant disadvantage if they lack access to similar data. However, they can level the playing field somewhat if they are able to trade in data with other firms, both by selling data they have collected from their customers and purchasing data collected by other firms. In theory, customers ought to benefit from the increased level of competition.[29]

Of course, collection and subsequent transfers of personal data can also generate costs, such as when collection is excessive and the protection of data or limitations on downstream uses are not sufficiently protected. The Cambridge Analytica scandal is an example of this, where lax information privacy practices by Facebook may have helped spread misinformation about presidential candidates, affecting the legitimacy of the U.S. election.[30]

Finally, data transfers can create costs for third parties. The simplest examples are when one person directly provides information about another person—for example by tagging their image in a photograph. People can also provide information about third parties indirectly. For example, anyone who shares information about their DNA simultaneously discloses information about the DNA of their biological relatives as well.[31] Similar consequences arise when interacting with "smart" products, such as smart speakers, smart cars, or other products where third parties' information may be recorded without their knowledge or control. More generally, when large numbers of people all share many different types of personal data, it becomes pos-

---

[28] *See Amazon Personalize*, AWS, https://aws.amazon.com/personalize (last visited May 6, 2019) (detailing Amazon's machine learning service for creating individualized product recommendations for customers); *Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (last updated Aug. 29, 2017) (outlining Amazon's consumer data collection policy, including Amazon's use of data to customize shopping recommendations).

[29] Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339, 355 (2017) (describing how data collector intermediaries can help firms overcome barriers to entry in data collection).

[30] *See* Omri Ben-Shahar, *Data Pollution* 10 (Univ. of Chi., Pub. Law Working Paper No. 679, 2018) (conceptualizing data harms as negative externalities and explaining how the Cambridge Analytica breach harms the broader public in addition to the exposed parties).

[31] *See* Frederick R. Bieber, Charles H. Brenner & David Lazer, *Finding Criminals Through DNA of Their Relatives*, 312 SCI. 1315, 1315 (2006) (discussing the use of DNA samples to identify close relatives of suspects).

sible to identify patterns in the data and draw inferences about people who have not shared data.[32] Transfers of data concerning third parties may merit special regulatory attention, particularly when they involve the imposition of costs. These kinds of third-party effects are generally beyond the scope of contract law. As such, they are beyond the scope of our inquiry here. We focus on relationships that are, or are capable of being, subject to contract.

C. Information Barriers

Rational market participants will only enter into transactions that they expect to make them better off. However, if they are poorly informed then there is no guarantee that their transactions actually will be beneficial, especially if they systematically underestimate costs or overestimate benefits.

Participants in markets for data often misunderstand the nature and consequences of their transactions. There are three main reasons for this.[33] First, collection, use, and transfer of data often are inherently difficult for consumers to observe. And after the initial collector has transferred the data to third parties, observation of subsequent use and transfer typically is nearly impossible. Consequently, consumers may misperceive the types of data being collected, how they are being used, or how widely they are being disseminated. These kinds of misperceptions can persist even in the face of explicit disclosures about the nature of the transaction.[34] Second, consumers may misperceive the impact that collection and dissemination of their col-

---

[32] For example, it appears to be possible to use images and data on sexual orientation collected from dating sites to predict the sexual orientation of people who have shared only their images. *See* Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images*, 114 J. PERSONALITY & SOC. PSYCHOL. 246, 250 (2018) (reporting that an algorithm accurately distinguished between gay and heterosexual men in eighty-one percent of cases, and in seventy-one percent of cases for women).

[33] *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2005, at 26, 29–31 (2005) (analyzing the role of incomplete information and bounded rationality in privacy-sensitive decisions); *see also* Acquisti, Brandimarte & Loewenstein, *supra* note 4, at 509 (discussing the information asymmetry arising from the invisible nature of the collection and use of personal data); Strandburg, *supra* note 4, at 96 (citing complications of advertising business models and the difficulty of predicting the harm from certain types of data collection).

[34] *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 47 (2014) (concluding that mandatory disclosures fail to produce the knowledge required to make informed decisions); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 29 (2014); Florencia Marotta-Wurgler, *Does Contract Disclosure Matter?*, 168 J. INSTITUTIONAL & THEORETICAL ECON. 94, 114 (2012).

lected data will have on their welfare. Some of these misperceptions obviously result from incomplete information, but that is not the only possible explanation. Third, people may display "bounded rationality" and psychological biases that prevent them from analyzing information they have received in a rational way.[35] For instance, the fact that the benefits of data transfer often are realized immediately while the costs are uncertain and will only be incurred in the future might trigger biases. These misperceptions that are specific to data transfers may be compounded by misperceptions that affect contracting behavior in many markets, such as tendencies to focus on relatively salient terms of an agreement and to overlook less salient terms. A growing body of empirical research supports many of these claims about both the existence and causes of these misperceptions.[36]

II
Special Contract Law for Data Transfer?

There is a great deal of interest in exploring how the legal system ought to regulate markets for data. Some of the most prominent theories focus on how law can preserve the economic benefits of markets for data while mitigating the effects of information barriers. As we shall see, some of the prescriptions call for deviations from conventional principles of contract law. These proposals either explicitly or implicitly challenge normative theories of contract law which call for the conventional principles to be applied universally. This Section begins by distinguishing universal and particularistic theories of contract law. It then explains how the principle that contract law ought to be designed to promote mutually beneficial transactions can be used to support particularistic theories of contract law. The next Section sets out the argument that information barriers justify a particularized approach to governance of transfers of personal data. We call this the information barriers theory. The final Section discusses objections to this information barriers theory.

A. Universalistic Versus Particularistic Theories of Contract Law

Contract law is the law of enforceable promises. A contract is simply a promise or set of promises that contract law will enforce, and contract law is the body of law which defines the circumstances in

[35] *See* Herbert A. Simon, Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization 198 (2d ed. 1957).

[36] *See, e.g.*, Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 Computers & Security 122, 130 (2017).

which one or more actors enjoy the right to enforce another actor's promise. Here we will focus on contracts that take the forms of promises to transfer data, possibly subject to restrictions on use or transfer, in exchange for something of value. For example: I promise to tell you the names of my customers in exchange for your promise to pay me $10,000, as well as your promises not to use the data to determine access to credit, insurance, or employment; not to resell the data; and to take precautions against unauthorized access. Contract law enforces both the promise to transfer the customer names and the promises regarding use, transfer, and security.

The substantive rules of contract law cover only a small number of topics: Which promises are enforceable (Formation, Excuses)? When does a promise need to be enforced (Interpretation)? By and against whom are promises enforceable (Privity)? What does it mean to enforce the promise (Remedies)? The procedural rules that govern resolution of contractual disputes are not usually considered to be part of "contract law."[37] However, those rules have such a large impact on the practice of making and enforcing promises that they are sometimes analyzed together with substantive rules of contract law.

Contract doctrine varies from one market to another, especially once we get beyond a few basic principles.[38] For example, in the United States, different parts of the Uniform Commercial Code (UCC) govern the contractual aspects of sales of goods (Article 2), leases (Article 2A), transfers of securities (Article 8), and loans secured by personal property (Article 9). Loans governed by real property are governed by still other doctrines that vary from state to state. Within each of these bodies of law there are often different rules for transactions that involve consumers and those that involve other types of parties. In addition, there are many markets in which private actors have opted out of state-provided rules and created their own industry-specific rules of contract law. Lisa Bernstein has famously

[37] *See* Robert E. Scott & George G. Triantis, *Anticipating Litigation in Contract Design*, 115 YALE L.J. 814, 818 (2006); *cf.* Kevin E. Davis & Helen Hershkoff, *Contracting for Procedure*, 53 WM. & MARY L. REV. 507, 511–15 (2011) (arguing that the ways in which parties contract for procedure in dispute resolutions require attention and oversight).

[38] As Brian Bix has pointed out, legal scholars sometimes describe contract law as though its main principles were universal, meaning that the same principles apply across all possible markets. Brian H. Bix, *The Promise and Problems of Universal, General Theories of Contract Law*, 30 RATIO JURIS 391, 392 (2017). Peter Benson, for example, begins his well-known analysis of contract law with an assertion that the main elements of contract law have been embraced "throughout most of the contemporary world." Peter Benson, *The Unity of Contract Law*, *in* THE THEORY OF CONTRACT LAW: NEW ESSAYS 118, 118 (Peter Benson ed., 2001); *cf.* Felipe Jiménez, Response, *Against Parochialism in Contract Theory: A Response to Brian Bix*, 32 RATIO JURIS 233 (2019) (documenting convergence in the contract law of common law and civil law jurisdictions).

documented the rules created by merchants who deal in diamonds, grain and feed, and cotton, and has explained how they diverge from the rules found in Article 2 of the UCC.[39] It is also well known that contract law varies across jurisdictions, especially between those with a common law and a civil law heritage.[40]

The variations in contract law across markets are not necessarily minor. There are deviations from even the most fundamental principles of the common law of contracts, including the principles that consideration is a pre-requisite to contract formation and that remedies for breach of contract are designed solely to compensate for the lost value of expected performance.[41] Consider, for instance, the law of our home jurisdiction, New York. The General Obligations Law dispenses with the requirement of consideration in transactions that involve transfers of securities,[42] but Article 9 of the UCC insists that consideration is a pre-requisite to enforceability for loan agreements secured by personal property.[43] Expectation damages are the ordinary remedy for breach of contract,[44] but damages for breach of a contract to provide medical services exclude non-economic losses such as pain and suffering.[45] At the same time, in New York, as in other states, breaches of certain consumer contracts may violate consumer protection statutes, which allow victims to recover damages equal to three times their loss, to a maximum of one thousand dollars.[46]

---

[39] Lisa Bernstein, *Merchant Law in a Merchant Court: Rethinking the Code's Search for Immanent Business Norms*, 144 U. PA. L. REV. 1765 (1996) (documenting rules used by arbitrators in the grain and feed industry); Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. LEGAL STUD. 115 (1992) (same, for the diamond industry); Lisa Bernstein, *Private Commercial Law in the Cotton Industry: Creating Cooperation Through Rules, Norms, and Institutions*, 99 MICH. L. REV. 1724 (2001) (same, for the cotton industry).

[40] *See, e.g.*, Mariana Pargendler, *The Role of the State in Contract Law: The Common-Civil Law Divide*, 43 YALE J. INT'L L. 143 (2018).

[41] Benson seems to presume that there is a consensus about these principles. Benson, *supra* note 38, at 131.

[42] N.Y. GEN. OBLIG. LAW § 5-1101 (Consol. 2018) ("An agreement, promise or undertaking for the purchase, sale, transfer, assignment or delivery of [specified types of debt, shares, or interests in stock], is not void or voidable, for want of consideration, or because of the nonpayment of consideration . . . .").

[43] N.Y. U.C.C. § 9-203(b) (Consol. 2018) ("[A] security interest is enforceable against the debtor and third parties with respect to the collateral only if: (1) value has been given . . . .").

[44] *See* Freund v. Wash. Square Press, Inc., 314 N.E.2d 419, 420–21 (N.Y. 1974) (stating that the law's purpose is to give the injured party the "benefit of his bargain").

[45] *See, e.g.*, Robins v. Finestone, 127 N.E.2d 330, 332 (N.Y. 1955) ("The damages recoverable in malpractice are for personal injuries, including the pain and suffering which naturally flow from the tortious act."); Mitchell v. Spataro, 452 N.Y.S.2d 646, 646 (App. Div. 1982).

[46] N.Y. GEN. BUS. LAW § 349(h) (Consol. 2018).

There is active debate over whether and to what extent the rules of contract law ought to vary across markets. Some normative theories of contract law purport to be universal, in the sense that they commend certain substantive rules of contract law for all markets. This is especially true of deontological theories, which derive principles of contract law from a small number of superordinate values, such as respect for individual autonomy. Randy Barnett, Peter Benson, and Charles Fried have all developed theories of this sort.[47] They all appear to suggest that contract law ought to universally embrace several key principles. For instance, they all seem to accept that a person should only be able to enforce a promise after they have assented to it and that the ordinary remedies for breach should be expectation damages or specific performance.[48]

In opposition to these universalistic theories stand particularistic theories that prescribe different rules of contract law for different markets.[49] The leading U.S. proponent of this kind of particularistic theory of contract law is probably Karl Llewellyn.[50] He argued that the law governing transactions between merchants should be different from the law for transactions involving non-merchants and that the law for dealings in houses should be different from the law for dealings in horses, which should in turn be different from the law for industrially manufactured goods.[51] He placed particular emphasis on

---

[47] CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION (2d ed. 2015) (arguing that the moral basis of contract law is the promise principle); Randy E. Barnett, *Contract Remedies and Inalienable Rights*, 4 SOC. PHIL. & POL'Y 179 (1986) (defending consent-based theory of contract with specific performance as primary remedy for breach); Benson, *supra* note 38, at 169.

[48] *See* FRIED, *supra* note 47, at 4; Barnett, *supra* note 47, at 184; Benson, *supra* note 38, at 119.

[49] A separate body of literature seeks to justify variations in contract doctrine across jurisdictions. *See, e.g.*, Aditi Bagchi, *The Political Morality of Convergence in Contract*, 24 EUR. L.J. 36 (2018) (discussing the importance of "national fit" in divergence of contract doctrines among European nations).

[50] In his synthesis of Llewellyn's theory of contract law, Alan Schwartz says, "Llewellyn did not ask what rule sellers and buyers in general would want, but rather what rule parties would agree to given their *particular* circumstances." Alan Schwartz, *Karl Llewellyn and the Origins of Contract Theory*, *in* THE JURISPRUDENTIAL FOUNDATIONS OF COMMERCIAL AND CORPORATE LAW 20 (Jody S. Kraus & Steven D. Walt eds., 2000).

[51] K.N. Llewellyn, *Across Sales on Horseback*, 52 HARV. L. REV. 725, 743–44 (1939) [hereinafter Llewellyn, *Across Sales on Horseback*]; K.N. Llewellyn, *The First Struggle to Unhorse Sales*, 52 HARV. L. REV. 873 (1939) [hereinafter Llewellyn, *Struggle to Unhorse*]. The issue of whether the 'law of the horse' ought to embody a distinct set of legal principles is distinguishable from the question of whether that body of law ought to be the focus of teaching and scholarship. The latter set of questions prompted a famous debate between Frank Easterbrook and Larry Lessig. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207–08; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999).

the idea that different types of agreements ought to be interpreted differently. For instance, he thought that an implied warranty of freedom from latent defects was not appropriate for the sale of a horse but was appropriate for the sale of an industrially manufactured good.[52]

With respect to data privacy contracts, there has been a strong push for a particularistic approach, as exemplified by the implementation of the GDPR, which dictates that firms adopt specific information practices and include particularized disclosures in their privacy policies; the American Law Institute's *Principles of the Law: Data Privacy*; and the scholarship of privacy expert Paul Schwartz.[53]

B. Economic Justifications for a Particularistic Approach to Contract Law

Particularistic theories tend to be instrumental as opposed to deontological in orientation. In other words, they are premised on the notion that contract law ought to be designed to promote specific objectives. The most prominent theories focus on how contract law can facilitate mutually beneficial exchanges, including by overcoming information barriers. Contract law generally plays a critical role in facilitating mutually-beneficial exchanges that cannot be concluded instantaneously because performance either takes time or is difficult to verify.[54] In these cases, one party must take the risk of beginning to perform its side of the bargain or investing in reliance on the promise before it can be sure that the other party will complete performance. Knowledge that the promise can be enforced helps to mitigate this risk. For example, a sale of a list of customer names may only be mutually beneficial if the price paid by the purchaser is conditioned upon the authenticity of the names and the purchaser agrees that the names are solely for its own use and cannot be used to determine eligibility for credit, employment, or housing. However, it might take time for the purchaser to verify that the names on the list are not fakes. This means that either the seller must deliver the names before being assured that the purchaser will fulfill its promise to pay, or, alternatively, the purchaser must pay before being certain that the names are authentic as promised. Similarly, it will only become clear over time whether the purchaser has abided by the restrictions on use,

---

[52] *See* Llewellyn, *Across Sales on Horseback*, *supra* note 51, at 743–44; Llewellyn, *Struggle to Unhorse*, *supra* note 51, at 903–04.

[53] *See supra* note 9 and accompanying text.

[54] Anthony T. Kronman, *Contract Law and the State of Nature*, 1 J.L. ECON. & ORG. 5, 28 (1985) (summarizing the argument that contract law is a relatively low-cost device for reducing the transaction costs of exchange).

and so the seller must deliver the names without knowing whether the purchaser will comply. In each case, the prospect that the second-mover's promise will be enforced mitigates the risks associated with being the first mover. The prospect of enforcement also encourages a party to make costly investments designed to increase the value it will earn from the other party's anticipated performance. For example, knowledge that a seller's promise to transfer authentic data will be enforced might encourage a purchaser to hire a team of marketing analysts in advance of receiving the data.[55]

Different components of contract law support exchanges in different ways. For instance, formation rules can be used to induce parties to deliberate before entering into contracts, hopefully helping them to recognize and avoid disadvantageous transactions. In the consumer context, formation rules tend to focus on disclosure and reasonable notice to increase the likelihood that consumers are informed before they decide to take or leave the non-negotiable agreements presented to them.[56] Rules of contract interpretation can help parties to minimize the cost of drafting contracts by incorporating their preferred terms as defaults. For example, suppose that many parties would be best off if their agreements include restrictions on transfer, require the implementation of specific security measures, or prohibit the data from being used to determine eligibility for credit. Default rules that treat those restrictions as implied terms even when the agreement is silent will spare parties the trouble of drafting those restrictions and requirements and thereby minimize drafting costs for parties who want to include them in their agreements. Alternatively, default rules can be information-forcing, meaning that they can be used to educate uninformed parties about their options. These sorts of implied terms also serve to protect parties who either underestimate the risks associated with a transaction or are unaware of how to draft terms that will mitigate those risks. Finally, contract law's remedial rules determine the potency of incentives to abide by and rely upon contracts.

It should be evident from the above that the proposition that contract law ought to be designed to facilitate mutually beneficial exchanges is highly compatible with particularistic theories of contract

---

[55] *Cf. id.* at 5 ("From the point of view of the parties themselves, the law of contracts is a valuable and important institution because it enables them to harness the state's power of coercion for their own private ends."). *See generally* Hermalin, Katz & Craswell, *supra* note 23, at 7–56 (providing an overview of the economic motive for contracts).

[56] *See, e.g.*, Melvin A. Eisenberg, *Disclosure in Contract Law*, 91 CALIF. L. REV. 1645, 1674 (2003) (proposing a seller's duty to disclose information, even if deliberately acquired, because of their asymmetric access to information, among other reasons).

law. On this approach, the appropriate rules for any given market will vary depending on factors such as the distribution of preferences among the participants. The rules that best promote mutually beneficial transactions will also depend on the level of information barriers. As we shall see, this idea can be used to justify the adoption of special rules to govern markets for personal data.

C. Special Contract Law for Data Transfer?

There is a widespread view that markets for personal data are dysfunctional and that special legal measures, meaning interventions that involve significant deviations from ordinary principles of contract law, are required to correct the problems. Some of these proposals are motivated by concerns about how transfers of personal data affect third parties.[57] Others are motivated by non-instrumental considerations.[58] Our focus here is exclusively on proposals designed to respond to the information barriers that confront consumers with a view to promoting mutually beneficial transactions.

Many aspects of the law of contracts can be used to eliminate or mitigate the effects of information barriers. To begin with, it may be useful to adjust the rules on formation and enforceability. For instance, the enforceability of an agreement might depend on whether the data collector or transferee has taken affirmative steps to help the transferor understand its terms and ramifications. Much of the aforementioned "Notice and Choice" regime articulated by the FTC focuses on formation rules encouraging more salient and simpler disclosures. Like all disclosure rules, these are effective to the extent which they induce consumer readership and understanding.[59]

Implied restrictions on use or transfer can protect consumers who fail to appreciate the value of such restrictions. Even if collectors ask consumers to opt out of these terms, the implied terms might serve as penalty defaults, meaning that the process of seeking consent to the opt-out may prompt consumers to become more informed about the ramifications of their decision and seek more favorable terms.[60] For instance, an implied requirement that a data collector adopt security

---

[57] *See, e.g.*, Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014) (noting privacy harms posed by data mining to individuals who never consented to the use of their data and recommending a framework for redress).

[58] *See, e.g.*, Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 124 (2004) (positing "contextual integrity" as a normative approach to the protection of privacy based on theories of justice).

[59] *See supra* notes 33–34 and accompanying text.

[60] *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 91 (1989) (introducing the concept of

measures consistent with 'industry best practices' would encourage collectors who wish to adopt less stringent practices to say so explicitly, which might draw attention to the issue. If, however, there is a significant risk that consumers will be duped into opting out of implied terms, then it may be appropriate to make those terms mandatory as opposed to defaults.

According to the ordinary rules of privity of contract, agreed restrictions on use or transfer cannot be enforced against third parties to the contract.[61] Insistence on privity limits the effectiveness of contractual restrictions in scenarios where a claim against the initial transferee is insufficient to deter or provide compensation for breach—for instance, when that initial transferee is judgment proof. In order to facilitate enforcement, it may be useful to make restrictions on use or transfer binding on third parties to whom data are transferred, regardless of whether they have assented to them.[62] The tort of inducement of breach of contract serves this purpose by allowing liability to be imposed on a third party who, with notice of a contract, induces its breach.[63] The doctrine could, however, be extended to third parties who lack notice or to agents and employees who advise a third party to induce breach.

It may also make sense to deviate from the ordinary rules governing rights to terminate contracts and to sue for breach. Broad rights to terminate agreements protect transferors from agreements that they belatedly recognize as disadvantageous. Meanwhile, in cases of breach, injured transferors who find it difficult to prove the magnitude of their losses can be given liberal access to forms of specific relief, such as deletion of data, designed to restore them to the position they were in before the contract was formed. As for damages, the expectation damages default forces the breaching party to pay damages equal to the harm it has caused.[64] A prominent justification for this rule is that it gives promisors an incentive to take efficient precautions against breach, that is to say, any precautions which cost less

---

penalty default rules that parties have an incentive to contract around and thereby reveal information to each other or to third parties).

[61] *See* 9 TIMOTHY MURRAY, ET AL., CORBIN ON CONTRACTS § 41.2 (2018) (defining privity).

[62] *Cf.* Molly Shaffer Van Houweling, *The New Servitudes*, 96 GEO. L.J. 885, 889–91 (2007) (arguing for the application of a property-based servitude framework to assess restrictions binding third parties in the context of software and other intangible property).

[63] *See* RESTATEMENT (SECOND) OF TORTS §§ 766–67 (AM. LAW INST. 1979).

[64] *See* RESTATEMENT (SECOND) OF CONTRACTS § 347 (AM. LAW INST. 1981) (defining expectation damages).

than the harm they are expected to avert.[65] However, if the losses from breaches of data transfer contracts are difficult to detect, prove, or ascertain, then the incentive effects of the expectation damages rule will be diluted. Suppose, for example, a promisor expects only one in ten breaches to result in detection and liability. In this case, the expectation damages rule only creates an incentive to invest in precautions that cost one-tenth the amount of harm likely to be caused by a breach. To create optimal incentives, it will be necessary to award higher, supracompensatory damages.[66] A particular problem in the information privacy space is that many harms that arise from the improper disclosure or use of personal data are dignitary in nature and hard to characterize under the existing rubric of recoverable harms, leading many cases to be dismissed for lack of standing or recoverable damages.[67] An expansion of what constitutes a recoverable harm would increase the likelihood that promisors internalize all harms stemming from breach.

Finally, the procedural rules that govern resolution of contractual disputes can also encourage enforcement. The most obvious examples of enforcement-friendly rules are those permitting collective proceedings such as class actions, which allow the costs of enforcement to be shared by multiple parties.

Paul Schwartz's model of "propertized personal information" is a prominent example of a proposal to modify the rules of contract law in order to address the information barriers that confront consumers engaged in data transfers.[68] Schwartz characterizes his model as a set of ideas for reform of property rights in personal data, but it also clearly implicates core questions of contract law.[69] The property law aspect of Schwartz's proposal would force potential data collectors to

---

[65] Melvin A. Eisenberg & Brett H. McDonnell, *Expectation Damages and the Theory of Overreliance*, 54 HASTINGS L.J. 1335, 1336 (2003); *see also* Richard Craswell, *Contract Remedies, Renegotiation, and the Theory of Efficient Breach*, 61 S. CAL. L. REV. 629, 646 (1988) (defining the formula for an efficient level of precaution).

[66] The precise level of damages required to create optimal incentives for precautions is difficult to calculate. One reason is that the probability of detection is difficult to observe and may vary from one context to another. The probability of detection is also a function of the level of damages because the higher the level of damages, the greater the incentive parties have to invest in learning about their rights and whether they have been violated. *See generally* Richard Craswell, *Deterrence and Damages: The Multiplier Principle and Its Alternatives*, 97 MICH. L. REV. 2185, 2193–94 (1999) (discussing why probability of punishment might vary with defendants' behavior and implications for calculating fines that will achieve optimal deterrence).

[67] *See* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. (forthcoming 2019) (manuscript at 4).

[68] Schwartz, *supra* note 2, at 2059, 2100.

[69] *See id.* at 2058.

obtain consent to collect, use, or transfer personal data.[70] In other words, it would clarify that data subjects enjoy property rights in personal data. However, Schwartz's proposal also includes several elements that would modify conventional principles of contract law: the ability to insist on adequate notice prior to authorization of privacy practices;[71] implied restrictions on use or transfer of personal data beyond the initially authorized category of use;[72] the ability to enforce restrictions on use or transfer against third party transferees of the data;[73] rights to withdraw from the contract;[74] statutory damages for breach of privacy promises;[75] and rights to pursue class actions for breaches.[76] It is reasonably clear from Schwartz's presentation that these rules would all be mandatory rather than default rules.[77]

Some aspects of this approach to regulation of data transfer are reflected in the American Law Institute's *Data Privacy Principles*, of which Schwartz is a co-Reporter.[78] For example, the *Principles* dictate different notice or consent requirements depending on the type of information being collected and processed, thus violating the principle that contract law ought to be neutral in relation to the subject matter of transactions.[79]

The GDPR takes a similar approach.[80] Most obviously, the GDPR attempts to address information barriers by requiring "data controllers" to obtain consent to data processing "in an intelligible and accessible form, using clear and plain language."[81] They must also inform "data subjects" about how their data will be used, how long the data will be kept, and how they can exercise their data-related rights.[82] If the controller intends to transfer personal data to a non-EU

---

[70] *Id.* at 2103.

[71] *See id.* at 2102.

[72] *See id.* at 2098.

[73] *See id.* at 2112 (advocating for data trading laws that include private rights of action).

[74] *See id.* at 2106.

[75] *See id.* at 2108.

[76] *See id.* at 2112.

[77] *See id.* at 2096.

[78] *Data Privacy*, ALI ADVISER, http://www.thealiadviser.org/data-privacy (last visited June 25, 2019).

[79] *See* PRINCIPLES OF THE LAW: DATA PRIVACY § 4(5)(a) (AM. LAW INST., Tentative Draft No. 3, 2018) (setting forth requirements for heightened notice applicable to "any data activity that is significantly unexpected or that poses a significant risk of causing material harm to individuals").

[80] *See, e.g.*, GDPR, *supra* note 12, art. 9 (outlining different requirements for processing special categories of personal data revealing information such as racial origin, religious beliefs, and political opinions); *id.* art. 99 (stating when the GDPR will go into effect).

[81] *Id.* art. 7(2).

[82] *Id.* art. 13.

country, this information should be included in the privacy policy.[83] In addition, controllers need to disclose any third parties who will handle the data.[84] In the event of an unauthorized transfer of data (i.e., a data breach) that creates "a high risk to the rights and freedoms of natural persons," the data controller must notify the subject.[85] All of this information must be provided in concise, clear, and plain language.[86] These rules fit within the known disclosure paradigm and are compatible with a contractual approach.

The GDPR also imposes restrictions on use and transfer. Personal data can only be retained for as long as necessary to fulfill the original basis for collection and processing.[87] Specifically, it mandates implementation of "appropriate" security measures and permits data subjects to sue for compensation for violations of its provisions.[88] Data subjects are also entitled to rectification of inaccurate personal data.[89] As for transfers following the initial collection, the GDPR requires transfers from data controllers to processors to be governed by a written contract that gives the controllers significant control over the processor's activities, requires consent for data transfers to subprocessors, and requires compliance with the GDPR.[90] With regard to enforcement, the GDPR effectively permits data subjects to terminate agreements by withdrawing their consent to processing.[91] Although it does not refer to U.S.-style supra-compensatory damages or class actions, the GDPR does encourage collective enforcement by giving data subjects the right to mandate a non-profit to conduct enforcement proceedings on their behalf.[92]

In contrast to previous regimes seeking to affect exchanges involving information privacy, such as the FTC's 2012 Privacy Guidelines and the OECD Fair Information Principles, which embrace a self-regulatory approach,[93] the GDPR gives enforcement

---

[83] *Id.* art. 13(1)(f).

[84] *Id.* art. 13(1)(e).

[85] *Id.* art. 34(1).

[86] *Id.* art. 12; *see also* Shmuel I. Becher & Uri Benoliel, *Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR*, *in* CONSUMER LAW & ECONOMICS (Klaus Mathis & Avishalom Tor, eds., forthcoming 2019) (manuscript at 2) (on file with the *New York University Law Review*) (analyzing whether privacy agreements subject to the GDPR are indeed readable).

[87] GDPR, *supra* note 12; art. 5(1)(e).

[88] *Id.* arts. 5(1)(f), 25, 32, 79, 82.

[89] *Id.* arts. 5(d), 16.

[90] *Id.* art. 28.

[91] *Id.* art. 7(3).

[92] *Id.* art. 80.

[93] *See* FED. TRADE COMM'N, *supra* note 11, at 13–14; ORG. FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 17 (2013).

agencies the authority to impose significant sanctions for violations, including up to four percent of a company's yearly global revenues.[94] This creates a marked distinction between this regime and all previous ones.

Finally, a striking feature of EU law, which predates the GDPR, is the way in which it attempts to circumvent both the constraints of privity of contract and the traditional limitations on extraterritorial jurisdiction to deal with situations in which EU residents' personal data are transferred outside of the EU. The GDPR specifically authorizes transfers of this sort when the transferor enters into an agreement with the transferee that incorporates the protections provided under EU law and allows the data subject to enforce those rights as a third-party beneficiary of the agreement.[95]

D. Objections to the Information Barrier Theory

We call the argument that information barriers justify the adoption of special rules to govern transfers of personal data the "information barrier theory." That theory has proven to be quite influential, but it is far from uncontestable.[96] In fact, it rests on several premises that may not be universally valid.

First, the theory assumes that information barriers cannot easily be surmounted. This may not be true. Just as data collection technology continues to advance, so does technology that allows people to control the ways in which data are being collected from them. For instance, widely available software allows Internet users to prevent either publishers of the websites they visit or third parties such as advertising companies from collecting data on subsequent browsing

---

[94] *See* GDPR, *supra* note 12, arts. 83, 84 (giving EU Member States the authority to determine appropriate penalties to impose for violations of the GDPR while setting maximum fines for certain violations).

[95] *Id.* art. 46(2)(c)–(d) (permitting transfers without specific authorization if governed by standard data protection clauses); Commission Decision 2010/87 of Feb. 5, 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, annex, 2010 O.J. (L 39) 11 (establishing a standard third-party beneficiary clause); Commission Decision 2004/915 of Dec. 27, 2004, Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, annex, 2004 O.J. (L 385) 79 (same).

[96] The discussion in this Section focuses on economic objections to the information barriers theory and associated policy prescriptions. There are other possible grounds for objection, such as concerns about paternalism. *See generally* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013) (discussing costs and benefits of allowing people to consent to collection and use of personal data).

activity.[97] Application Programming Interfaces (APIs) in mobile platforms offer another example: Consumers are now often asked to give permissions regarding the collection and use of information by the application.[98] In light of this arms race, it might be premature to declare victory for collectors in the battle to control the flow of personal data. In addition, relatively unsophisticated consumers may learn about possible restrictions on transfer by observing terms offered to more sophisticated parties. Finally, it is worth emphasizing that imperfect information is not necessarily an obstacle to mutually beneficial exchange. Information barriers are mainly of concern when they lead to underestimation of costs or overestimation of benefits. These kinds of misperceptions may become less likely as consumers become more aware—in a general sense as opposed to in relation to specific transactions—of the potential consequences of transfers of personal data. For all these reasons, consumers may actually have more access to more information than the information barrier theory would presume.

A second premise of the information barrier theory is that a significant number of consumers strongly prefer to impose restrictions on use or transfer of data collected from them. Although individuals often report to researchers that they place relatively high values on restrictions designed to protect their personal data from further dissemination, their behavior often suggests that they place lower values on those restrictions—the so-called "privacy paradox."[99] Moreover,

---

[97] *See* Hanqing Chen, *Privacy Tools: How to Block Online Tracking*, PROPUBLICA (July 3, 2014, 9:00 AM), https://www.propublica.org/article/privacy-tools-how-to-block-online-tracking (describing three common ways Internet users can block trackers from collecting their data).

[98] This might have been influenced by the Federal Trade Commission's effort to simplify mobile disclosures. *See, e.g.*, FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15–18 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[99] Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100, 101, 108–13 (2007) (defining the privacy paradox as the gap between consumers' stated intentions to disclose personal information and their actual disclosure and providing evidence from a study intended to confirm and explain its existence); *see also* Acquisti, Brandimarte & Loewenstein, *supra* note 4, at 509 (describing people's uncertainty over their own privacy preferences, the context-dependent nature of privacy preferences, and the malleability of privacy preferences); Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* 2 (Nat'l Bureau of Econ. Research, Working Paper No. 23488, 2017) (describing the results of study analyzing causes of privacy-decreasing behaviors); Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks*, 2005 PROCS. ACM WORKSHOP ON PRIVACY ELECTRONIC SOC'Y 71, 77 (2005) ("We can conclude that only a

the values that people place on these restrictions vary significantly depending on contextual factors, such as whether the restrictions are framed as improvements or declines from the status quo.[100]

Third, the theory assumes that the benefits from imposing restrictions on use or transfer exceed the costs associated with inducing parties to incorporate those restrictions in their agreements. However, those costs might be substantial. If the potential uses and users of a given type of data are difficult to foresee at the time of the initial transfer, then the benefits that might flow from exploiting new valuable uses and users either will be lost entirely or diminished in the process of renegotiating the original restrictions. The costs associated with restrictions that bind third parties who acquire data without notice may be especially large. If these kinds of third-party restrictions are possible, everyone interested in acquiring data has an incentive to incur the cost of investigating whether any prior transfer has created binding restrictions on use or transfer. Naturally, the magnitude of those costs will depend significantly on the technology used to publicize the restrictions.

A fourth contestable premise of the information barrier theory is that specific forms of private litigation, such as class actions, are critical to ensuring enforcement of restrictions on use or transfer. However, reputational sanctions and public enforcement also can lead to

---

vanishingly small number of users change the (permissive) default privacy preferences."); Kokolakis, *supra* note 36, at 130 (summarizing various attempts to explain the privacy paradox); Kevin Lewis, Jason Kaufman & Nicholas Christakis, *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. COMPUTER-MEDIATED COMM. 79, 95 (2008) (finding that a third of college students using Facebook changed their default privacy settings); Dan Svirsky, *Why Are Privacy Preferences Inconsistent?* 14 (Harvard Law Sch. John M. Olin Ctr. for Law, Econ., & Bus., Discussion Paper No. 81, 2019) (finding further evidence that preference inconsistency and information avoidance, where consumers prefer not to find out or make choices, contribute to the privacy paradox). There is also research showing that individuals will claim that they value their privacy, only to give it up for very small amounts of money soon after. *Cf., e.g.*, Alessandro Acquisti, Leslie K. John & George Lowenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 267 (2013) (finding that, though more than half of the participants in a study were unwilling to give up privacy in order to gain an extra two dollars, the overwhelming majority of participants were unwilling to pay two dollars in exchange for increased privacy); Leslie K. John, Alessandro Acquisti & George Loewenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONSUMER RES. 858, 868 (2010) (showing that people's privacy concerns are influenced by contextual clues often unrelated to the actual risks of disclosure); Adam S. Chilton & Omri Ben-Shahar, *Simplification of Privacy Disclosures: An Experimental Test* 4–5 (Univ. of Chi. Law Sch. Coase-Sandor Working Paper Series in Law & Econ., No. 737, 2016) (finding that simplifying privacy disclosures did not change users' behavior).

[100] *Cf.* Kokolakis, *supra* note 36, at 125 (describing an experiment which found that customers were willing to pay more to protect their private information only when the options to protect and not to protect the information were presented together).

sanctions for breach of restrictions on use or transfer.[101] In principle, the deterrent effects of these kinds of sanctions may be sufficient to obviate the need for private litigation, at least for those losses that are salient to consumers.

III
An Empirical Examination of the Information Barriers Theory

The information barriers theory, like other instrumental theories of contract law, can, at least in principle, be examined empirically. To begin with, we can assess the potential value of the flexibility afforded by the contractual approach by examining differences in information privacy practices across markets. Variations across markets may suggest that different parties find different restrictions on use and transfer of data mutually beneficial in different contexts. For instance, firms that collect less sensitive data might offer weaker protections. Such a finding would suggest that mandating higher levels of protections would discourage a certain number of mutually beneficial transactions, assuming of course that the weaker protections do not result from the exploitation of information barriers and do not result in unacceptable net costs for third parties.

We can also examine parties' agreements for indications that information barriers are impeding mutually beneficial exchanges.[102]

---

[101] *Cf.* Strandburg, *supra* note 4, at 156–57 ("Reputation is not an effective mechanism for screening for credence goods, such as data collection, however, since consumers cannot judge quality even after purchase."). For a discussion of the role of reputation in disciplining firms, see generally Clayton P. Gillette, *Rolling Contracts as an Agency Problem*, 2004 Wis. L. Rev. 679.

[102] There is a large empirical literature that analyzes the content of terms and contracting practices to examine whether regulation might be necessary in a number of areas, ranging from transactions between large and sophisticated parties to consumer transactions, including markets for personal data. *See generally* Zev J. Eigen, *Empirical Studies of Contract*, 8 Ann. Rev. L. & Soc. Sci. 291 (2012). In the context of privacy policies, see, for example, Ian Reay, Scott Dick & James Miller, *A Large-Scale Empirical Study of P3P Privacy Policies: Stated Actions vs. Legal Obligations*, 3 ACM Transactions on the Web 6:1, 6:2 (2009), which conducts a large scale empirical study of privacy policies and finds that a large fraction failed to comply with the mandatory rules of the privacy laws of their respective countries; Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. Legal Stud. S163, S182 (2016), which finds that many terms in privacy policies, especially those of unregulated companies, are ambiguous and difficult to interpret; Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. Legal Stud. S69, S87, S93 (2016), which finds that courts and laypeople show a different understanding of the terms in privacy policies and concludes that there is little reason to expect the development of a robust market for premium privacy-protective email applications in the United States. For similar studies in the context of other consumer contracts, see, for example, Florencia Marotta-Wurgler, *Competition and the Quality of Standard Form Contracts: The Case of Software License*

Specifically, we can compare the practices of parties who face varying levels of information barriers over time. We can examine whether transactions that involve data collection from parties who face low barriers to information adopt a) the same kinds of restrictions as parties who appear to face higher information barriers and b) the kinds of restrictions and enforcement provisions favored by proponents of the information barriers theory. If the two groups converge on similar terms, then the assumption that they have different levels of access to information might have to be revisited. Another possibility is that some or all of the restrictions adopted by the more informed parties diverge from those recommended by proponents of the information barrier theory. This finding would call other components of the theory into question. For instance, it might suggest that for some parties the costs associated with restrictions outweigh the benefits.

This kind of analysis is complicated by the fact that a number of factors besides information barriers affect contracting behavior. Three broad categories of factors are particularly worthy of note: 1) the characteristics of the parties and their relationship, including their objectives, relative amounts of information (other than information

---

Agreements, 5 J. EMPIRICAL LEGAL STUD. 447, 467–73 (2008), which finds that, while firms in more competitive markets offered lower prices, there was no difference in the quality of terms offered by firms in such markets; Florencia Marotta-Wurgler, *What's in a Standard Form Contract? An Empirical Analysis of Software License Agreements*, 4 J. EMPIRICAL LEGAL STUD. 677, 703 (2007), which finds that terms in end user license agreements were not always maximally exploitative relative to the default rules of Article 2 of the UCC. *See also* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 553 (2014) (proposing that the FTC should require sellers to confirm consumers' expectations of the terms in their contracts and to affirmatively warn consumers about unfavorable terms); Meirav Furth-Matzki, *On the Unexpected Use of Unenforceable Contract Terms: Evidence from the Residential Rental Market*, 9 J. LEGAL ANALYSIS 1, 2–4 (2017) (studying the use of unenforceable contract terms in the context of residential leases); Florencia Marotta-Wurgler & Daniel Svirsky, Do FTC Privacy Enforcement Actions Matter? Compliance Before and After US-EU Safe Harbor Agreement Actions 4–6 (Aug. 2, 2016) (unpublished manuscript) (on file with the *New York University Law Review*) (finding that firms including terms in privacy policies that were in violation of several privacy regulations were unlikely to revise those terms even after the FTC brought enforcement actions for similar violations against other firms, thus questioning the deterrent effect of enforcement actions). In the corporate context, see, for example, MITU GULATI & ROBERT E. SCOTT, THE THREE AND A HALF MINUTE TRANSACTION: BOILERPLATE AND THE LIMITS OF CONTRACT DESIGN 33–44 (2013), which explores theories of what makes contract terms "sticky"; Marcel Kahan & Michael Klausner, *Standardization and Innovation in Corporate Contracting (or "The Economics of Boilerplate")*, 83 VA. L. REV. 713 (1997), which examines how learning benefits and network effects may result in parties using inefficient contract terms; Michael Klausner, *Corporations, Corporate Law, and Networks of Contracts*, 81 VA. L. REV. 757 (1995), which examines how network effects may inefficiently slow changes in terms; John C. Coates IV, *Why Have M&A Contracts Grown? Evidence from Twenty Years of Deals* 2 (Harvard Law Sch. John M. Olin Ctr. for Law, Econ. & Bus., Discussion Paper No. 889, 2017), which finds that merger agreements show high degrees of innovation.

about the implications of the transaction), and available opportunities; 2) the characteristics of the parties' contracting environments, and, in particular, the contractual terms that have been adopted by other similarly situated parties; and 3) the applicable law.

Variations in party characteristics, the contracting environment, and applicable law can either generate or mask differences between the contracting practices of more and less informed parties. For example, suppose we observe that restrictions that bind third parties are more prevalent among more informed parties. At first glance, this finding appears to support the information barriers theory—information barriers prevent parties from adopting value-enhancing terms. However, the finding is also consistent with the possibility that the informed parties in the study value these restrictions because they have greater capacity to monitor and sue third parties, but parties with less capacity would not derive as much value from the restrictions. Another possibility is that the informed parties adopt these provisions as part of a wasteful competition to signal their trustworthiness and would be better off if the law prohibited this kind of costly signaling. Or perhaps the parties' contracting behavior is explained primarily by forces that pressure them to adopt standardized documents, and the fact that informed parties converged on agreements with stringent restrictions on data transfer is merely a historical accident. Yet another possibility is that the informed parties in our study are systematically more likely to be subject to the EU's GDPR, which mandates adoption of various kinds of third-party restrictions, including in cases involving transfers of personal data outside the EU.[103]

Conversely, suppose that both more and less informed parties converge on agreements that include limitations on damages. At first glance this finding seems to contradict the information barriers theory—there is no evidence that information barriers prevent anyone from adopting value-enhancing provisions for supracompensatory damages. However, an alternative explanation is that both groups have been thwarted in their effort to adopt value-enhancing terms, but by different obstacles: Less informed parties have been blocked by information barriers while more informed parties have yielded to pressure to conform to existing standard form documents.

A final concern stems from the fact that we can only observe the terms of data collectors' standard written agreements. We cannot observe any specially negotiated amendments to those agreements,

[103] This kind of extraterritorial influence on the part of EU law would be an example of what Anu Bradford calls the "Brussels Effect." Anu Bradford, *The Brussels Effect*, 107 Nw. U. L. Rev. 1, 3 (2012).

nor, generally, can we observe whether the firms' actual behavior conforms to the written terms. This is another potentially significant limitation of our analysis. There are at least two reasons to conjecture that these kinds of deviations from standard terms are more likely to affect sophisticated parties. First, sophisticated parties are more likely to be aware of opportunities to negotiate for amendments to, or exemptions from, standard terms. Second, sophisticated parties are more likely to enjoy the bargaining power required to induce firms to deviate from standard terms.[104]

That being said, there might be some parties who are sophisticated enough to become informed and understand the privacy implications of the agreements, but not sufficiently large to extract any special treatment from the data collectors. This is especially true for one market we study: cloud computing. While there are large institutions, like NYU, which are likely able to contract with Google or Dropbox for special terms or are likely to ignore the standard terms and negotiate a custom arrangement if anything goes wrong, there are many other smaller firms who shop carefully for the cloud computing service firm that offers the best protections and terms, as stated in their standard terms. We examine whether the terms offered to such firms by data collectors differ from those offered to ordinary consumers.

In the remainder of this Part we summarize the results of an empirical analysis of the terms of privacy policies. The first Section describes our dataset. The following Section describes trends over time in those policies, taking into account the impact of the GDPR. The next Section describes variations across markets in order to shed light on whether firms value the flexibility afforded by the contractual approach. The final Section explores the impact of information barriers by comparing terms offered to more and less sophisticated customers in the cloud computing market.

A. Data

We begin with a subset of 194 privacy policies from firms contracting with U.S.-based consumers for seven online markets where consumers often share personal data: adult (17 firms), cloud computing (17 firms), dating (31 firms), gaming (19 firms), news and reviews (15 firms), social networks (33 firms), and special interest message boards (42 firms). These are markets where data transfer is a

[104] For general discussions of reasons why parties' practices might deviate from standard terms, see Gillette, *supra* note 101, at 703–06, who suggests that firms are likely to deviate from standard terms for consumers whom they judge to be behaving reasonably.

relatively salient aspect of the contractual exchange. There are also differences in the nature of privacy concerns across these markets. Individuals share more or different personal data on social network sites as compared to gaming sites. Indeed, the services offered by dating and social network sites depend on personal data shared by users. Other markets involve activities that are highly private (in the case of adult sites), or involve significant losses in the event of, for example, a security lapse or equipment failure (in the case of cloud computing). For each of these firms, we collected the privacy policy in 2014 and in August of 2018, after the enactment of the GDPR. We start with an analysis of the whole sample of policies and then turn to market differences later.

The firms involved do business in the United States, but most also have overseas operations. They include the largest firms, such as Amazon and Google, and many smaller firms. The sample selection process is described in detail in Marotta-Wurgler's previous study.[105] The privacy policies in this study are those offered to individuals situated in the United States. Table 1 summarizes company, service, and policy characteristics.

[105] *See* Marotta-Wurgler, *supra* note 10, at S22–26.

TABLE 1. SUMMARY STATISTICS. N=194 companies for which the privacy policy was available in both 2014 and 2018. Company characteristics include dummy variables for nonprofit and public ownership. Product characteristics include whether the user must pay and the popularity of the website according to Alexa.com (lower numbers mean more popular). Privacy policy characteristics include a dummy for a claim of certification to one or more standards, the year the policy was last updated (not available for all policies), and the length of the policy.

		2014	2018
Nonprofit (0 - 1)	mean	0.05	
Public (0 - 1)	mean	0.27	
Paid Service (0 - 1)	mean	0.43	
Alexa Rank	mean	453,227	1,216,821
	median	4,514	22,003
	min	1	1
	max	10,000,000+	10,000,000+
Certification is Claimed (0 - 1)	mean	0.28	0.2
Year Last Updated	N	135	148
	mean	2011	2017
	median	2012	2018
	min	2005	2006
	max	2014	2018
Number of Words	mean	2,177	4,099
	median	2,137	2,907
	min	9	9
	max	9,368	47,153

About five percent of the firms in the sample are nonprofits. These may be structurally different, which could affect information privacy practices. Twenty-seven percent of the sample firms are public, which we use as a proxy for firm size and sophistication. Firms' business models might also have an effect on information privacy practices, so we track for that. Forty-three percent of sample firms offer at least a portion of their services for a fee, but there are differences across markets. Over ninety percent of dating sites, a little over half of cloud computing and gaming sites, and a quarter of all adult sites are offered on a subscription basis. The remaining markets do not offer subscriptions but offer premium access or the ability to purchase items for a price.

Alexa ranking is a ranking of websites from Alexa.com and is based on the estimated average number of daily unique visitors and

the estimated number of page views during the past three months.[106] We use this measure as an additional proxy for firm size and reputation, as well as the potential volume of personal data flow. We also use this measure to ensure that the sample firms are representative of each market. A lower number indicates a more popular site; Google, YouTube, and Facebook have Alexa rankings of 1, 2, and 3, respectively. For the firms in our sample, the mean Alexa rank in 2014 was 453,227 (median 4514) and 1,216,821 (median 22,003) in 2018. The difference in ranking is caused by Alexa's reporting of only world rankings in 2018, but U.S. rankings in 2014. Almost 30% of firms in 2014 adopted a code of conduct in the form of privacy seals, such as TRUSTe, or the U.S.-EU Privacy Shield. This number dropped to 20% in 2018, perhaps due to a substitution effect, likely created by the GDPR.

On average, contracts in force in 2014 were last updated in 2011 (median 2012). The mean date of last update is 2017 for the sample contracts collected in 2018, while the median date of last update is 2018. Indeed, the majority of firms updated their contract, even though the ones we track govern non-E.U. citizens, around the time when the GDPR came into effect. The date of last updates sheds some light into the influence of the GDPR on the sample firms' privacy policies. This might explain why the average number of words almost doubled, from 2177 in 2014 to 4099 in 2019. The median length of contracts was 2137 words in 2014 and 2907 words in 2018.

As explained in Marotta-Wurgler's 2017 study, each contract was read and its terms coded by hand by pairs of law students working independently, so that each contract was coded twice.[107] Some judgments needed to be made because contracts often include ambiguous clauses and give rights that cannot be exercised. For example, consumers are commonly told that they are given a choice as to how their personal data can be shared, but they are not told how that choice can be exercised and they do not appear to be offered the choice outside the contract. In these instances, we did not code these promises since we had clear evidence that contractual promises did not track actual practices.

B. Impact of the GDPR

We are interested in examining empirically the extent to which contracts might adequately allow for exchange of personal data by evaluating variations in thirty-eight terms related mostly to security

[106] *See About Us*, ALEXA, https://www.alexa.com/about (last visited May 10, 2019).
[107] *See* Marotta-Wurgler, *supra* note 10, at S22.

practices, over time—from 2014 to 2018—as well as within and across markets. To do this we must first account for the possibility that some terms may have changed to comply with the GDPR. For this reason, we divide these terms into those that are implicated by the GDPR (which thus may have affected their substance) and those that are not. This will allow us, in a crude way, to attempt to isolate contracting practices that are relatively unaffected by special regulation.

Table 2 tracks the content of the sample privacy policies in 2014 and 2018 and evaluates the relative degree of compliance of each term with GDPR requirements, and measures the difference over time.

TABLE 2. PRIVACY POLICIES AND THE GDPR, 2014 VERSUS 2018. Fraction of firms whose privacy policy contains terms consistent with the GDPR. Terms are grouped by categories: Contextual Integrity, Data Accuracy Safeguards, Data Breach, Data Retention, Notice Privacy by Design, Processor Contracts, Security Measures, Sharing Consent, User Control * denotes a statistically significant change at the 10% level in a two-sided test.

		N	2014	2018	Change
Contextual Integrity	PII used only for stated, context-specific purposes (e.g., user would expect that this data would be shared for service to function)	192	0.27	0.28	0.01
Data Accuracy Safeguards	Guarantees data accuracy	192	0.02	0.03	0.01
	Company adopts reasonable procedures to ensure accuracy	192	0.32	0.1	-0.22*
Data Breach	User will be notified of any data breach	192	0.04	0.07	0.03
Data Retention	Provides notice of data procedures if company is sold or otherwise ceases to exist	190	0.07	0.52	0.45*
	User given a choice of what happens to data if company is sold or otherwise ceases to exist	193	0.02	0.06	0.04*
	States time limit for data retention (including when account is closed)	194	0.06	0.16	0.1*
	Personal data are destroyed or anonymized when account is closed	194	0.08	0.48	0.4*
	Data are protected under same policy (or destroyed or anonymized) if company ceases to exist	194	0.14	0.23	0.09*
Notice	Recipients of shared or sold data are identified	191	0.1	0.14	0.04
	Words such as "affiliates" or "third parties" are defined, if used	156	0.06	0.11	0.05
Privacy by Design	Describes substantive privacy and security protections incorporated into operating procedures (e.g., limiting number of employees with access to data)	194	0.44	0.28	-0.16*
Processor Contracts	Affiliates and subsidiaries are bound by the same privacy policy	113	0.19	0.53	0.34*
	Contractors (e.g., payment process companies) are bound by the same privacy policy	143	0.19	0.54	0.35*
	Third parties are bound by the same privacy policy	143	0.05	0.15	0.1*
	Company reports performing due diligence to ensure legitimacy of third parties that have access to data	186	0.02	0.2	0.18*
	Company has contract with third parties establishing how disclosed data can be used	146	0.12	0.42	0.3*

Security Measures	Identifies means of technological security (e.g., encryption)	194	0.43	0.47	0.04
	Has a procedure for safely disposing of unused data	193	0.02	0.09	0.07*
	Does not disclaim liability for failure of security measures	194	0.41	0.22	-0.19*
	Requires periodic complicance review of structural and technological data security measures	194	0.11	0.07	-0.04*
	Contains self-reporting measures in case of privacy violation (to a privacy seal organization, third-party consultant)	194	0.04	0.05	0.01
Sharing Consent	Opt-in consent mechanism for sharing/selling PII or sensitive information (except for typical internal business purposes)	108	0.38	0.09	-0.29*
	Opt-in or opt-out consent mechanism for sharing/selling non-PII or sensitive information to non-service providers (except for typical internal business purposes)	194	0.1	0.14	0.04
User Control	User allowed to access and correct personal data collected	194	0.63	0.77	0.14*
	User can request that information be deleted or anonymized	191	0.53	0.68	0.15*
	MEAN	180	0.19	0.27	0.08*

The terms are divided among ten categories loosely based on the areas of information privacy practices related to use, sharing, data security, and enforcement, as presented in the GDPR: Contextual Integrity (a term which ensures that personally identifiable information be collected and used consistent with context specific purposes), Data Accuracy Safeguards (two terms that require the company to take precautions in ensuring data are accurate), Data Breach (a term that requires collectors of data to notify subjects in the event of breach), Data Retention Practices (five terms related to data retention, anonymization, and deletion protocols, as well as polices for when the entity is acquired or ceases to exist), Notice (two terms related to the identifications of recipients of the collected data), Privacy by Design (a term tracking whether the firm commits to implementing privacy and security protections in the operation of the firm), Processor Contracts (five terms tracking whether the collector ensures that third party processors of the data will take adequate precautions regarding data security), Security Measures (five terms tracking the extent to which the collector safeguards the information adequately), Consent Mechanisms for Sharing Personal Information (two terms tracking the subject's choices regarding sharing with third parties), and User Control (two terms tracking whether the subject can access and correct his or her own information, or request that it be deleted or anonymized). The terms we track do not cover *all* the terms outlined in the GDPR. Rather, they focus on those information pri-

vacy practices that relate to sharing, contextual integrity, security, and enforcement. We focus on these terms because they are the ones that received the most attention and have been the source of multiple cases and scandals related to consumer information privacy. Thus, these are the terms most likely to become relevant in the event of a problem.

The first column of the table highlights each category and the terms within it. The findings are in the rightmost columns, which reports compliance levels for each term in 2014 and 2018 and documents the change and its statistical significance. Overall, there has been an increase in the promised level of protection over the sample period, with firms offering an increased number of security protections in 2018 (with 27% of GDPR-compliant security-related terms), from 19% in 2014, a statistically significant increase. While the focus of this paper is not on evaluating the extent to which firms comply with data privacy guidelines or mandatory rules, it is important to note that, while the overall level of compliance is not high in absolute terms (perhaps because the terms do not perfectly align with the GDPR and because the contracts we track are not necessarily governed by its requirements, as they govern U.S. consumers), the average level of compliance for all sample terms, and for some in particular, is high as compared to documented levels of compliance with non-binding guidelines, such as those of the FTC.[108]

Focusing on individual categories of terms yields some interesting findings. Overall, twenty-one of the twenty-eight terms became more protective over the sample period, and ten of those did so in a statistically significant manner. For example, 77% of firms now allow subjects to access and correct their personal data, a significant increase from 2014. More strikingly, while only 8% of firms made a commitment to destroy or anonymize personal data upon account or service termination in 2014, 48% did in 2018. Processor Contracts is the category with the most improved protections: Firms barely contracted with data processors and third-party recipients of data to protect subjects' data in 2014, yet this changed drastically in 2018, as the policies now describe various ways in which subsequent transfers of data are protected by contract. Not all terms became more protective, however. Five turned in the other direction over time, all of them in a statistically significant manner. These include terms related to ensuring data accuracy, privacy by design, disclaiming liability for

[108] *See* Florencia Marotta-Wurgler, Understanding Privacy Policies: Content, Self-Regulation, and Markets 4 (Mar. 1, 2017) (unpublished manuscript) (on file with author) (finding the average sampled policy complied with only thirty-nine percent of the 2012 FTC guidelines).

security measures, and providing opt-in (as opposed to opt-out) options for the sharing of sensitive information. While it is impossible to derive any normative or efficiency related conclusions, especially because we weigh each term equally, we document a clear increase in protection of subject personal data for those terms that are subject to the GDPR.

Of course, these increased protections are more meaningful when consumers can enforce them and seek legal redress. In addition, these can be enforced by public authorities, such as the FTC or State Attorneys General. Table 3 documents the changes in dispute-resolution terms over the sample period.

TABLE 3. REDRESS TERMS, 2014 VERSUS 2018. Terms are defined so that a value of 1 is more pro-privacy, consistent with other tables.

	N	2014	2018	Change
No choice of forum specified	194	0.21	0.3	0.10*
No choice of law specified	193	0.13	0.17	0.04*
No arbitration clause (or consumer may choose)	194	0.74	0.56	-0.18*
No class action waiver	194	0.79	0.62	-0.17*
No disclaimer of liability for failure of security	194	0.41	0.23	-0.18*
MEAN	194	0.46	0.38	-0.08

Choices of law and forum have become less pervasive over the sample period, with a 10% statistically significant decrease in choice of forum clauses by 2018. These have been offset, however, by almost 20% increases in arbitration clauses and class action waivers, and an 18% increase in disclaimers of liability for security measures. Given the magnitude of individual losses, the increase in class action waivers may have a non-trivial impact in consumers' ability to seek redress. In addition (non-reported), 52% of firms disclaim damages or limit them to the purchase price, a practice consistent with other industries. It is important to note that, even in cases where consumers can seek class remedies under rights given under the contract, courts have overwhelmingly dismissed cases alleging breaches of information privacy promises because of a failure to articulate or prove any harm recoverable in law.[109]

[109] *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132 & n.2 (2011) (explaining that courts will only award compensation for "cognizable" or

C. Changes Independent of the GDPR

Table 4 tracks the change in seven security, sharing, and contextual integrity-related terms, among others, that are not covered by the GDPR.

TABLE 4. NON-GDPR TERMS, 2014 VERSUS 2018. Fraction of firms whose privacy policy contains various pro-privacy terms. Fraction is calculated on firms for which term is applicable and have a policy in both the 2014 and 2018 sample. * denotes a statistically significant change at the 10% level in a two-sided test.

	N	2014	2018	Change
Third parties may not place advertisements that track user behavior	194	0.15	0.1	-0.05*
Company does not reserve right to disclose protected information to comply with the law or prevent a crime	194	0.16	0.11	-0.05*
Company does not reserve right to disclose protected information to protect own rights	194	0.29	0.18	-0.11*
User will be given notice of government requests for information about the user	193	0.03	0.03	0
Provides contact information for privacy concerns or complaints	193	0.93	0.93	0
Provides link to FTC's Consumer Complaint Form and/or its telephone number	193	0.1	0.02	-0.08*
Claims privacy seal, certification, or consistency with an industry oversight organization's practice	194	0.28	0.2	-0.08*
MEAN	194	0.28	0.22	-0.06*

Contracting parties arguably have more freedom to define these terms than the ones reported in Table 2. The first column lists the terms, which include: whether third parties can place ads tracking user behavior; whether the firm states that it will disclose data to cooperate with law enforcement or to prevent a crime, or protect its own rights; whether the firm provides contact information where consumers can report privacy concerns or complaints; and whether the firm adheres to a privacy certification organization, such as TRUSTe, among others. All terms but two, which remained the same, became less pro-

"material" harms); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018) (explaining that plaintiffs will not succeed if they cannot show harm regardless of whether defendants were at fault).

tective over the sample period. These changes were all statistically significant.

On first impression, one might conclude that terms that were subject to the GDPR got better, while those that were not got worse. Yet there are important subtleties that complicate the picture. For example, while it is true that a significant number of firms now do not adhere to a certification or seal, this is likely due to a crowding out effect of the GDPR. The same is true of the decline in the number of firms providing a link to the FTC's consumer complaint form. It is also the case that we only track seven terms and that other terms in privacy policies that also are not subject to the GDPR may have become more protective. Still, for terms related to security and enforcement, those not subject to the GDPR became slightly less protective relative to the two benchmarks we use. Is contracting, then, compromised by information barriers?

D. Variations Across Markets

Table 5 explores this question more closely by splitting the privacy policies by market and repeating the analysis shown in Table 2.

TABLE 5. PRIVACY POLICIES BY MARKET, 2018. Analysis of 2018 policies of N=196 firms. For each category of terms, we compute the average consistency with the GDPR across terms, then across firms within that market. To maximize the sample size, firms are not required to also have a 2014 policy available. Terms are grouped by categories: Contextual Integrity, Data Accuracy Safeguards, Data Breach, Data Retention, Notice, Privacy By Design, Processor Contracts, Security Measures, Sharing Consent, User Control. A "+" ("–") denotes statistical significance greater (less) than other markets at the 10% level.

	Adult (N=19)	Cloud Computing (N=17)	Dating (N=31)	Gaming (N=19)	News and Reviews (N=15)	Social Networks (N=53)	Software as Service (N=2)	Special Interest Message Board (N=42)
Contextual Integrity	0.52+	0.35	0.19	0.05-	0.13	0.32+	0	0.31
Data Accuracy Safeguards	0.05	0.12	0.02	0.16+	0.07	0.07	0.25	0.05
Data Breach	0	0	0.03	0.05	0.07	0.06	0	0.21+
Data Retention	0.31	0.32	0.32	0.35	0.25	0.31	0.5	0.2-
Notice	0.08	0.17	0.15	0.11	0.07	0.09	0.25	0.16+
Privacy by Design	0.58+	0.35	0.13-	0.21	0-	0.38	0.5	0.26
Processor Contracts	0.48	0.35	0.41	0.36	0.41	0.3-	0.55	0.28-
Security Measures	0.30+	0.27+	0.14-	0.17	0.17	0.17	0.4	0.16
Sharing Consent	0.08	0.15	0.05	0.05	0.03	0.21+	0	0.08
User Control	0.68	0.85+	0.77	0.66	0.67	0.76	0.75	0.64

For each category of terms we compute the average consistency with the GDPR across terms, then across firms within each market.

We also examine whether a particular market is more (or less) protective than other markets at a statistically significant level. The results are quite interesting: While Table 2 revealed that firms increased the level of data protection for GDPR-related terms, these levels vary across markets in fairly intuitive ways, consistent with what one would expect from market forces. These variations have remained constant across time, even after accounting for the GDPR.

Firms in adult and cloud computing, which tend to handle personal data that are deeply sensitive and valuable, are more likely than all other markets to include terms with more protective security measures. Adult sites are also more likely to respect contextual integrity and include privacy by design measures. Social networks are more likely than most other markets to offer consent-sharing options and to adopt contextual integrity collection and use practices. A possible implication of these findings is that firms in various markets might benefit from the flexibility that conventional principles of contract law afford. It is also telling that compliance with the GDPR, which is mandatory for firms handling data of citizens of EU member states (which includes most firms in the sample and might affect a subset of firms' global data practices), also varies across markets in consistent ways. While our methodology cannot measure GDPR compliance with one hundred percent accuracy (since we cannot measure actions beyond the contract and do not track GDPR compliance exhaustively, though we closely approximate this for the categories of terms that we track), the differences in compliance across markets suggest that market forces (and thus the desirability of the contractual approach) are still very much at play even in a mandatory regime.

Of course, some of the differences that we observe may reflect market failures stemming from information barriers. This is more likely to be the case in some of the sample markets. Dating sites, for example, are less likely to adopt privacy by design and security measures, maybe because these aspects of the service are not salient to consumers.

E. Variations Across More and Less Sophisticated Subjects

Finally, we explore the information barriers theory by comparing the security practices of firms in the cloud computing market that offer their services not only to consumers but also to professionals as well as small, medium, and large firms (unreported). First, we note that some firms that offer their services to various types of users do not offer identical terms to all. For example, Google and Dropbox include a promise of confidentiality for enterprise users but do not do

so for individual consumers who obtain the product for free or subscribe to options with little storage.[110] Yet both firms offer the same disclaimers of liability to all parties as well as the same privacy policies. One explanation for this difference is that large business customers might require a promise of confidentiality to hand over their valuable information, which likely includes trade secrets and client lists. Consumers might have different needs. Terms offered along a number of common categories are similar for consumers, professionals, and large firms. Though more research is needed to fully address this question beyond the firms we study here, this finding questions traditional stories of exploitation, at least with respect to this particular set of terms in this particular market. The takeaway is that we need to explore this more to fully conclude that it is only consumers who need protection relative to business users.

Conclusion

On the whole, our results suggest that regulation might play a role in setting a floor in terms of sharing, security, and contextual integrity protections. Still, given the intuitive variations across markets, there is arguably a case for traditional contract law, given the many benefits it offers in terms of flexibility and adaptability. The picture is complex, but desirable regulation might involve some mandatory rules ensuring minimal protections combined with the flexibility of contract. We need to learn more about information privacy practices across markets to craft the right types of rules.

The empirical analysis also has broader implications for the study of contract law and law reform. Specifically, it underscores the potential for divergence between instrumental and non-instrumental theories of contract law. First, in the context of markets for data, the prescriptions associated with the two classes of theories diverge in terms of both their particularity and their substance. Instrumental theories can easily support claims that principles of contract law ought to vary significantly across markets. They also can support claims that in some contexts the principles of contract law ought to deviate significantly from conventional principles. In any given context, the appropriate principles will depend on factors such as the subject matter of

[110] *Compare Dropbox Privacy Policy*, Dropbox (May 25, 2018), https://www.dropbox.com/privacy#business_agreementl (for businesses, Dropbox "won't sell [information] to advertisers or other third parties"), *and Google Cloud Platform Terms of Service*, Google Cloud (Nov. 2, 2018), https://cloud.google.com/terms (for businesses, Google "will not disclose the Confidential Information" except in limited situations), *with Google One Terms of Service*, Google One (Oct. 1, 2018), https://one.google.com/terms-of-service (allowing Google to share individuals' confidential information).

the transaction, the characteristics of the parties, their contracting environment, and, possibly, the legal rules adopted by other jurisdictions. By contrast, other normative theories of contract law favor universal application of conventional principles.

A second and related point is that instrumental and noninstrumental theories typically differ in terms of how they can be validated. Instrumental theories of contract law, like the information barriers theory, tend to be contingent on the validity of specific, empirically testable assumptions. It is valuable to test the empirical assumptions that underlie those theories, particularly if they point to radical departures from conventional principles. Our analysis demonstrates the feasibility of such tests.

Third, our analysis has implications for the design of the institutions that administer contract law. Many conventional theorists of contract law valorize the common law and courts' efforts to develop it.[111] In our view, however, the formulation of contract law ought to involve ongoing development and testing of hypotheses about how alternative principles are likely to affect the behavior of contracting parties in various markets. Courts involved in formulating principles of contract law to govern transfers of personal data might benefit from the assistance of other institutions such as administrative agencies, legislatures, and the American Law Institute.

Finally, our results suggest that the GDPR had a meaningful impact on information privacy practices as revealed in privacy policies but that firms across markets exhibited marked differences in compliance, thus suggesting that the flexibility of the contractual approach might be valuable in this highly innovative setting.

---

111 *See* Alan Schwartz & Robert E. Scott, *The Political Economy of Private Legislatures*, 143 U. PA. L. REV. 595, 596 (1995) (analyzing how private lawmaking organizations—the American Law Institute and the National Conference of Commissioners on Uniform State Laws—promulgate restatements of the common law); Samuel Issacharoff & Florencia Marotta-Wurgler, *The Hollowed Out Common Law* 2 (N.Y. Univ. Sch. of Law Pub. Law & Legal Theory Research Paper Series, Working Paper No. 18-33, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3261372 (analyzing how to identify the common law that governs modern commercial, electronic transactions).