2017

Contracting Over Privacy: Introduction

Omri Ben-Shahar

Lior Strahilevitz

CHICAGO

COASE-SANDOR INSTITUTE FOR LAW AND ECONOMICS WORKING PAPER NO. 792

COASE-SANDOR INSTITUTE
FOR LAW AND ECONOMICS
THE UNIVERSITY OF CHICAGO LAW SCHOOL

CONTRACTING OVER PRIVACY: INTRODUCTION

Omri Ben-Shahar and Lior Jacob Strahilevitz

THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO

January 2017

Contracting over Privacy: Introduction

Omri Ben-Shahar and Lior Jacob Strahilevitz

ABSTRACT

This short essay introduces papers presented at the symposium Contracting over Privacy, which took place at the Coase-Sandor Institute for Law and Economics at the University of Chicago in fall 2015. The essay highlights a quiet legal transformation whereby the entire area of data privacy law has been subsumed by consumer contract law. It offers a research agenda for privacy law based on the contracting-over-privacy paradigm.

1. INTRODUCTION

Big Data is an engine of profound changes in our society and a major stimulant of economic growth. Internet services that never existed, like searching, social networking, and online shopping, are now a source of major personal welfare. The Internet of Things transformed machines that used to provide simple static functionality into data-intensive personalized aids. Overall, data-driven services and devices are widely embraced by consumers.

These "smart" products are popular because they use the vast information network to help consumers improve usage and save money. But the firms that provide them also use the same data to determine people's interests and shopping profiles and then make money by selling personalized "behavioral" ads and additional products. A mobile GPS app that tracks people's location can help them get to their destinations more smoothly but also helps advertisers tailor location-specific ads. A tracking device that auto insurers offer to their policyholders can help price the policies more accurately and even reduce auto accidents and insurance premiums but also provides insurers a wealth of information about peo-

OMRI BEN-SHAHAR is the Leo Herzel Professor of Law at the University of Chicago Law School. LIOR JACOB STRAHILEVITZ is the Sidley Austin Professor of Law at the University of Chicago Law School.

[*Journal of Legal Studies*, vol. 45 (June 2016)]

ple's behavior, information that might be used in ways their customers do not expect.

In the era of technology-powered phones, cars, alarms, wallets, toothbrushes, and physical activity trackers, users' privacy has become a central regulatory preoccupation. Around the world, lawmakers are trying to keep up with the commercial data-collection enterprise and to secure basic rights for their customers, like the EU's "right to be forgotten" and its General Data Protection Regulation. In the United States, agencies like the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) have worked to tighten their oversight of firms' data practices. There is, however, a percolating sense among privacy advocates that the existing protective scheme is too weak, leaving too much freedom for firms to engage in surveillance and in monitoring of people and thereby to gain control over citizens' lives in a way that threatens their autonomy, intimacy, authenticity, and other important values. The fundamental question that these lawmakers and privacy advocates are asking is whether "contract" has gone too far to subsume privacy law. Has it become too easy for people to contractually waive privacy rights? Are people even aware that they are doing so? Should the freedom to contract over privacy be restricted?

2. THE ECONOMICS OF CONTRACTING OVER PRIVACY

The case for stricter regulation of firms' data privacy practices and the precise levers such regulation ought to deploy depend on the answer to a fundamental question: are markets failing to provide optimal privacy protection? In environments in which consumers care about their privacy, it might be thought that markets for data are the solution, not the problem. According to this standard line of thought, firms that want to lure consumers and prompt them to pay more for their services would promise their clientele greater privacy protection. In the same way that firms compete over warranties or the quality of customer service, data-driven firms could offer consumers privacy-protective platforms to gain a competitive edge. Firms have learned, for example, that offering customers no-contract arrangements (which allow early termination of the service without penalty) appeals to noncommitters. Firms could similarly offer no-prying arrangements to appeal to privacy seekers. Markets, rather than regulation, could potentially provide the desired privacy features.

Indeed, some Internet service providers are offering pay-for-privacy plans that cost more but involve no data collection and liberate the bounty-paying users from behavioral ads and privacy disturbances (Bode 2016).

There are several specific market mechanisms by which privacy might be regulated, rather than by the government. The primary one is contract. Since the privacy practices that firms employ are part of the contract between the firm and the consumer (often included in the terms of service), this contract becomes a platform for regulation of the parties' privacy rights. Consumers who give up some privacy receive in return something that they value more, often a price discount.

Regulation of privacy by contract occurs when firms promise to forgo otherwise available opportunities to use or collect personal information. They offer their customers a menu of choices, and people self-select. Like any other aspect of product quality, contracts can do the bulk of regulation—of creating and limiting rights. In the same way that people choose the duration of their service contracts, the coverage declarations of their insurance contracts, or the data package for their smartphones, they would choose their personally desired privacy rules. Public regulation is generally not necessary to establish mandatory durations, declarations, or data allocations, and it would similarly not be necessary in setting privacy protection.

This conclusion is rebutted if contracting involves negative externalities. There is some reason to think that choices about privacy and security could involve externalities, and the presence of these externalities ought to provide some basis for overriding personal preferences if the stakes are high enough (Allen 1999; Ayres 2016). For example, unraveling and related dynamics put significant pressure on people to keep up with others who publicize personal information (Schwartz 2004; Peppet 2011). Likewise, firms may not compete over data security if highlighting such aspects alerts otherwise uninformed consumers to new risks and dampens overall demand.

Another limit to contracting is transactions cost. Ordinarily, this concern suggests that law should play a relatively modest role of providing a set of privacy rights default rules. These privacy rights would govern the relationship between the firm and the client, but only in the absence of explicit contractual clauses on the matter. This is the gap-filling role that the law assumes in many other areas of contracting, and the main goal of preset default rules is to save the parties the hassle of expressly drafting them. The well-documented problem with this permissive regula-

tory approach is its weakness. Firms are able to override the substantive provisions embedded in the defaults by asking their customers to agree to a different set of terms. Thus, in an era in which most consumer transactions are accompanied by long predrafted standard-form agreements, and where it is exceedingly easy to elicit the consumer's assent to the terms, much of the regulation of privacy rights would be performed by contracts drafted in-house, not by laws that establish default rules.

Finally, efficient contracting faces informational and behavioral barriers. As in many areas of consumer contracting, the asymmetries in sophistication, knowledge, and stakes make it questionable whether consumers would effectively self-select into the packages of legal terms that best serve their heterogeneous interests. Unlike service durations, insurance declarations, or smartphone data allocations, privacy rights deal with matters that are not intuitive for consumers. It is enough to eyeball a typical privacy policy notice to realize that it governs mysterious issues: what type of information is being collected, how it is used, with whom it is shared, how long it is kept, and how it is protected. This complexity opens a fertile ground for the incorporation of behavioral factors into the understanding of privacy decision making (Adjerid, Samat, and Acquisti 2016).

Failures of imagination are widespread in privacy contracting because new and unanticipated uses of old data are constantly arising. Privacy policies are often written in ways that are truly confusing (Reidenberg et al. 2016). Further, these privacy policies also change over time (firms include a modification clause in the notice, which allows them to make such changes). And even if understanding one such policy is manageable, they come in battalions. Each website, financial arrangement, visit to a clinic, or new mobile app presents its own privacy practices. Any effort to master this accumulated complexity is infeasible, and any attempt to do so is irrational. According to one estimate, the average person encounters so many privacy disclosures every year that it would take 76 days to read them, and the lost time would cost the economy $781 billion (McDonald and Cranor 2008).

The complexity of contract terms dealing with privacy is a major obstacle for efficient private contracting. It poses a serious challenge for market regulation of privacy, but it may not be a fatal one. Privacy is not the only aspect of contracting that involves significant underlying complexity. Many other dimensions of consumer contracts are complicated but nevertheless bargained over and tailored to consumers' preferences.

Consumers do not understand the complexity of automobile mechanical design or the electronics that operate their laptops but are able to rely on market signals to make propitious choices. Their decisions are made manageable by various market-generated scores that aggregate the underlying loads of information and rate or rank the performance of the product and the satisfaction that similarly situated consumers derived from it. Such market indices foster competition over the otherwise complex and obscure features and thus complement the contract mechanism.

Accordingly, a central question for the contracting-over-privacy inquiry is the viability of privacy scores and ratings designed to simplify privacy choices. Some such tools are available, like the website PrivacyGrade.org or the TRUSTe privacy compliance certification. Yet, unlike ratings from *Consumer Reports* or *Zagat,* these privacy scores are not relied on heavily. Is it because, despite being counseled otherwise, people do not care much about their data privacy?

The answer is probably yes: most people do not care much about data privacy. When prompted by surveys, they might nod in agreement and announce that privacy matters, but when asked to pay for it, they are strikingly stingy. Some studies have found that people are willing to pay no more than a few dollars to prevent their apps from harvesting their smartphone data, no more than half a penny per search to make it private, and no more than $15 per year to avoid automated content analysis of their e-mail messages (Savage and Waldman 2013; Preibusch 2015; Strahilevitz and Kugler 2016). Maybe people will eventually learn to cherish their data privacy more, but at present the privacy tempest is in a teapot.

3. THE LAW OF CONTRACTING OVER PRIVACY

Contracting over privacy is of course permissible, but how do such contracts form? What is the legal status of privacy notices posted on websites, incorporated in mobile apps, or otherwise communicated to consumers? Surprisingly, this basic question has not received a simple and coherent answer in the privacy law commentary. The lack of definitive analysis has produced puzzling treatments by courts and unorthodox scholarly proposals.

This question of whether online privacy notices are contracts has created confusion in part because privacy law is longing for a different

notion of consent than general consumer contract law. Privacy law as a whole is a collage of legal doctrines from different areas, still struggling to identify the common underlying values and objectives (Kugler 2014). For example, a recent draft of the *Principles of the Law, Data Privacy* counts numerous sources for the regulation of privacy, what it calls "an interrelated amalgam of different types of law, including federal and state constitutional law, federal and state statutory law, tort law, evidentiary privileges, property law, contract law, and criminal law" (Schwartz and Solove 2016, intro. note, p. 1).

Privacy law has an uneasy relationship with contract. It has understandable ambitions to regulate a desirable baseline of privacy rights but a less coherent view of whether these rights can be waived. On the one hand, it is widely accepted that even when the law establishes baseline privacy rights, individual consent could modify them. Individuals, for example, could sell their rights by granting firms permission to collect, use, and share their personal information. This feature of the law appropriately accommodates heterogeneous preferences among subjects with respect to privacy and the associated tradeoffs. On the other hand, consent to standard-form contracts is hardly ever informed or meaningful, and it is hard to accept that such a passive ritual could undermine basic privacy entitlements.

Many of these issues are not unique to privacy rights. In other areas of contracting, courts have allowed passive assent to override pro-consumer legally enacted background rules. But what about privacy rights? Have they acquiesced to the same lenient contracting rules? Are consumers' clicks to "agree" sufficient to disclaim privacy rights? Many lawsuits for violations of privacy rights turn on the question of whether consumers truly consented to the standard-form contract terms that purport to grant the business the right to engage in its data practices. And yet the answer to this question is thought to be unsettled. It is often taught that privacy contracting is treated differently by courts than contracting over other matters (like warranties or arbitration). It is also thought that such differential treatment of privacy contracts is justified, because the guidelines concerning how to contract over privacy must come not from contract law but from privacy law.

As a result, despite the central role that consent has in establishing the scope of privacy rights, there is lingering confusion regarding the rules that govern the mutual assent to privacy terms. There is, for example, a prominent view that such rules must come from the doctrine of informed

consent in tort law rather than from consumer contract law (Schwartz and Solove 2014, sec. 4, comment A). Thus, rather than apply the ordinary rules of mutual assent—for example, the rule that determines how standard-form contracts are formed and what counts as sufficient disclosure—privacy scholars put their faith in privacy-specific consent rules and heightened notice requirements, which purport to apply only to agreements over data privacy (Schwartz and Solove 2014, secs. 3–4). In their view, "[t]he form by which consent is obtained must be . . . based on the type of personal data involved and the nature of the collection, use, or sharing of the personal data."

These heightened notice and assent requirements are inconsistent with first principles of contract law. In general, the doctrine of mutual assent requires parties to follow standard objective procedures, invariant to the content of the agreement. These procedures have evolved in the digital era, allowing standard contract terms to be adopted through relatively passive and spontaneous forms of agreement. But the assent rules are one and the same for all contracting matters—warranties, arbitration clauses, disclaimers, termination penalties—including privacy rights. Despite asymmetries between firms and consumers, courts apply the basic principle that individual assent overrides legally supplied protections and that the process necessary to contract around such default protections does not depend on their substance.

This principle—the content neutrality of contract formation doctrine—is overwhelmingly adhered to by courts. Its inverse—the idea that courts ought to adopt privacy-specific contracting rules—is likewise overwhelmingly rejected. A recent survey of all privacy disputes that reached court judgment paints a telling picture (Bar-Gill, Ben-Shahar, and Marotta-Wurgler 2016). Despite a holding by one court in the earlier days of the Internet that "broad statements of company [privacy] policy do not generally give rise to contract claims" (*Dyer v. Northwest Airlines,* 334 F. Supp. 2d 1196, 1200 [D.N.D. 2004])—a precedent that privacy scholars have taken as authoritative in describing the state of the law (see, for example, Solove and Schwartz 2011; Solove and Hartzog 2014)—the law has shaped up quite differently. To date, among 51 cases in which courts addressed this issue, only in five cases did courts decide that privacy notices are not contracts. All the remaining cases treated privacy notices as contracts. While most of these cases are unpublished federal district court cases, the conclusion is crystal clear: privacy policies are typically recognized and enforced as contracts.

What are the legal implications of the classification of privacy notices as enforceable consumer contracts? For firms, the contractual nature of privacy notices ensures two beneficial functions. First, privacy notices are deployed to shield firms against liability for data privacy practices that, absent consumer consent, would violate privacy laws. For example, absent consent, Gmail's practice of scanning contents of users' e-mail messages would be a violation of the Wiretap Act, and Facebook's practice of identifying users in uploaded photos would be a violation of state privacy laws. The contractual status of privacy notices means that users grant consent to these practices and thus provide firms a critical safe harbor.

The second function that privacy notices perform is the assurance for consumers that some uses of the data, which are otherwise permissible even without consent, would not occur. For example, firms and websites may keep logs of customers' activity, but they can promise in their privacy notices not to do so. If privacy notices are contracts, such promises are binding, and their breach would be actionable. Moreover, the FTC can (and does) treat breaches of these promises as deceptive trade practices. Avowing such potential liability is a credible way for firms to entice hesitant consumers to engage with them. Firms dealing with sensitive content, like adult websites, indeed make explicit and clear promises to limit data sharing with third parties, and cloud-computing sites make explicit promises to follow stringent data security standards (Marotta-Wurgler 2016).

The contractual nature of privacy notices has significant implications for lawmakers working to design statutory privacy protections. The first implication is for the design of default rules. If statutory privacy rights are merely default rules, lawmakers should anticipate wholesale opt outs. Firms that develop business models that are constrained by statutory privacy rules would post privacy notices that effectively override these rules.

The powerful incentives of firms to induce their customers to give up their privacy rights also suggests that the choice between opt-in and opt-out schemes is of less importance than people usually assume. Opt-in schemes are thought to be more protective, because they require firms to get consumers' affirmative consent to override the pro-consumer status quo. Opt-out schemes, by contrast, put the burden on consumers to initiate the exit from the pro-business status quo. Recent FCC regulations, for example, present the shift to an opt-in regime as a meaningful step toward more privacy protection, as this regime requires consumers' explicit consent before collecting sensitive data such as geographical location or

financial information. But firms are very good at getting consumers to opt in when doing so furthers the businesses interest (Willis 2013), and businesses are able to ask consumers repeatedly to change their minds if they initially resist information sharing. If indeed firms elicit such consumer consent with great ease, the opt-in framework makes little difference.

Once again, consumers may so easily agree to opt in, or fail to opt out, because of lack of information. Informed consumers might refuse to opt in or might initiate their own opt outs. These consumers would walk away from firms that refuse to provide the statutory privacy protections that they demand. Uninformed consumers, by contrast, would stick with any default rule. In such an environment of imperfect information, designing optimal default rules has to account for two separate concerns. First, it has to recognize that there are consumers who do care and who would seek to opt out of an undesirable default rule. For some, the default rule could be insufficiently protective, and they would look for more protection. For others, it would be too protective, and they would prefer to waive the protection for a price discount. These opt outs create transactions costs (the cost of becoming informed about the default rule as well as the cost of contracting around it), and a well-designed default rule has to minimize such costs. But the design of the default rule has to recognize, in addition, that many consumers would remain uninformed about the default rule and refrain from opting out, regardless of its content. For this group the default rule is sticky, and it ought to be designed with an eye to maximizing the value of the transaction. This is a general insight into the optimal design of default rules in consumer contracts: it has to meet two criteria—minimizing the cost of opt outs and maximizing the value of transactions when opt outs do not occur (Bar-Gill and Ben-Shahar 2016).

An additional implication of the contractual nature of privacy notices is the role of disclosures. Contracts over privacy—like any other consumer standard-form contract—are often long and complex. Is there a way to make such contracts simpler? Can the law require firms to present consumers pared-down versions of these privacy notices that would effectively inform consumers of the privacy risks? These questions have risen to the fore of consumer protection law in many areas, as regulators and commentators spend much effort to design simpler, smarter, and user-friendlier disclosures. In the privacy area, the proposals to utilize best practices in the presentation of privacy notices have been widely embraced, and more radical suggestions to use "nutrition facts"–type warn-

ing boxes are also intuitively advocated. But would such efforts have the desired effect on informing consumers' choices? There is some evidence that the answer is no (Ben-Shahar and Chilton 2016) and that the use of the privacy notice to engender trust may be limited (Martin 2016).

In the end, then, the law and economics of contracting over privacy differs only in detail, but not in principle, from the law and economics of consumer contracts. Courts overwhelmingly treat them in the same way, and for good reasons. Consumers' consent may be ill-informed, but regulatory alternatives might be worse. Consumer contract law has tools to combat overreaching by firms, and these tools—rather than superfluous notions of heightened disclosure or informed consent—ought to guide privacy protection. Such tools allow courts to strike down intolerable provisions, and in a separate article we propose to deny firms the advantages that they bury in cryptic boilerplate (Ben-Shahar and Strahilevitz 2016).

Accordingly, the papers from the symposium Contracting over Privacy collected in this issue examine general questions of contract formation, design, interpretation, and extracontractual norms and trust—all in the context of privacy. Privacy is not sui generis; it is instead a valuable laboratory to examine the evolution of contract law in the digital era.

REFERENCES

Adjerid, Idris, Sonam Samat, and Alessandro Acquisti. 2016. A Query-Theory Perspective of Privacy Decision Making. *Journal of Legal Studies* 45:S97–S121.

Allen, Anita L. 1999. Coercing Privacy. *William and Mary Law Review* 40:723–57.

Ayres, Ian. 2016. Contracting for Privacy Precaution (and a Laffer Curve for Crime). *Journal of Legal Studies* 45:S123–S136.

Bar-Gill, Oren, and Omri Ben-Shahar. 2016. Optimal Defaults in Consumer Markets. *Journal of Legal Studies* 45:S137–S161.

Bar-Gill, Oren, Omri Ben-Shahar, and Florencia Marotta-Wurgler. 2016. Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts. *University of Chicago Law Review* 83 (forthcoming).

Ben-Shahar, Omri, and Adam Chilton. 2016. Simplification of Privacy Disclosures: An Experimental Test. *Journal of Legal Studies* 45:S41–S67.

Ben-Shahar, Omri, and Lior Jacob Strahilevitz. 2016. Interpreting Contracts via Surveys and Experiments. Unpublished manuscript. University of Chicago Law School, Chicago.

Bode, Ken. 2016. AT&T Charges Steep Premium for Privacy, Calls it a "Discount." *DSL Reports,* March 17. https://www.dslreports.com/shownews/ATT-Charges-Steep-Premium-for-Privacy-Calls-it-a-Discount-136511.

Kugler, Matthew B. 2014. Affinities in Privacy Attitudes: A Psychological Approach to Unifying Informational and Decisional Privacy. Unpublished manuscript. Northwestern University, Pritzker School of Law, Chicago.

Marotta-Wurgler, Florencia. 2016. Self-Regulation and Competition in Privacy Policies. *Journal of Legal Studies* 45:S13–S39.

Martin, Kristen. 2016. Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online. *Journal of Legal Studies* 45:S191–S215.

McDonald, Alecia M., and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Privacy for the Information Society* 4:540–65.

Peppet, Scott R. 2011. Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. *Northwestern University Law Review* 105:1153–1203.

Preibusch, Soren. 2015. The Value of Web Search Privacy. *IEEE Security and Privacy* 13(5):24–32.

Reidenberg, Joel R., Jaspreet Bhatia, Travis D. Breaux, and Thomas B. Norton. 2016. Ambiguity in Privacy Policies and the Impact of Regulation. *Journal of Legal Studies* 45:S163–S190.

Savage, Scott, and Donald M. Waldman. 2013. The Value of Online Privacy. University of Colorado, Department of Economics, Boulder.

Schwartz, Paul M. 2004. Property, Privacy, and Personal Data. *Harvard Law Review* 117:2055–2128.

Schwartz, Paul M., and Daniel J. Solove. 2014. *Principles of the Law, Data Privacy*. Tentative draft no. 2, October 24. American Law Institute, Philadelphia.

———. 2016. *Principles of the Law, Data Privacy*. Council draft no. 1, September. American Law Institute, Philadelphia.

Solove, Daniel J., and Woodrow Hartzog. 2014. The FTC and the New Common Law of Privacy. *Columbia Law Review* 114:583–676.

Solove, Daniel J., and Paul M. Schwartz. 2011. *Privacy Law Fundamentals.* 2d ed. Portsmouth, NH: International Association of Privacy Professionals.

Strahilevitz, Lior Jacob, and Matthew B. Kugler. 2016. Is Privacy Policy Language Irrelevant to Consumers? *Journal of Legal Studies* 45:S69–S95.

Willis, Lauren E. 2013. When Nudges Fail: Slippery Defaults. *University of Chicago Law Review* 80:1155–1229.