Indiana Law Journal

Volume 98 | Issue 1 Article 2

Winter 2022

Illusory Privacy

Thomas Haley
University of Virginia School of Law, thaley@law.virginia.edu

Illusory Privacy

THOMAS D. HALEY*

For decades, regulators, consumer advocates, and privacy theorists have grappled with one of privacy's most important questions: how to protect private information that consumers unwittingly give away with the click of an "I accept" button. Reform efforts remain mired in a morass of text, focusing on the increasing volume and complexity of firms' terms of service and privacy policies. This Article moves beyond such existing approaches. By analyzing terms of service and privacy policies from hundreds of top websites—which this Article calls "platform terms"—this Article demonstrates that the prevailing "notice and consent" paradigm of privacy regulation cannot provide meaningful protection.

This Article centers platforms' unconstrained power as the flaw in notice-and-consent approaches. It makes three contributions to the contracts and privacy literatures. First, it explores the nuanced relationship between platform terms and contract law. Neither scholars nor courts agree on whether platform terms, and in particular privacy policies, constitute contracts. This Article shows that, in either case, both courts and regulators resort to contract reasoning to implement notice-and-consent approaches to privacy regulation. Second, it demonstrates that platforms enjoy complete authority over every aspect of their relationship with individuals. It explores the prevalence of unilateral modification provisions that obviate initial consent and remove any incentive for platforms to compete on terms. Platforms, software, and devices are also subject to unilateral change. Moreover, the trend toward industry consolidation likewise changes the party in possession of individuals' data. This paradigm leaves consumers with things they did not bargain for, on terms they did not accept, in a relationship with a party they did not choose. Third, this Article contends that there can be no workable notice-and-consent approach to privacy protection. In light of the amorphous relationship between individual and platform, only direct regulation of platforms' data collection, use, and transfer has the potential to protect individual privacy.

---

* Research Assistant Professor, University of Virginia School of Law. For helpful comments and conversations, I am grateful to Omri Ben-Shahar, Hannah Bloch-Webha, Danielle Citron, Kristen Eichensehr, George Geis, G. Mitu Gulati, Woodrow Hartzog, Andrew Hayashi, David Hoffman, Aziz Huq, Cathy Hwang, Christina Koningisor, Brian Leiter, Michael Morse, Christopher Morten, Aisha Saad, Alicia Solow-Niederman, Lior Strahilevitz, Ari Ezra Waldman, and Jacob Victor. Thanks to Emily Abbott, Hannah Comeau, and Virginia Johns for excellent research assistance.

INTRODUCTION

On January 14, 2021, Google completed its acquisition of wearable fitness-tracker company Fitbit, obtaining a panoply of highly sensitive health data about tens of millions of Fitbit users in the process.[1] Consumers who objected to Fitbit's transfer of their heart rate, menstruation, and sleep-pattern data to one of the world's most notorious data harvesters had little recourse, if they even knew the acquisition took place: Fitbit's Privacy Policy expressly permitted Fitbit to transfer consumer information in the event of "a merger, acquisition, or sale of assets."[2] That these users likely never read the Privacy Policy, or the terms and conditions that affirm the user's agreement to the Privacy Policy, is of no legal significance.

Terms and conditions, privacy policies, cookie policies, and the like—which this Article calls "platform terms"—are ubiquitous in modern life. In litigation, they operate as both sword and shield, forming the basis of claims for breach of contract and defenses of consent. Courts, in turn, regularly hold that they are enforceable contracts and even apply contract law in cases that do not turn on the terms'

1. Rick Osterloh, *Google Completes Fitbit Acquisition*, THE KEYWORD (Jan. 14, 2021), https://blog.google/products/devices-services/fitbit-acquisition/ [https://perma.cc/PF8E-HPD8]; Brent Rose, *Everything You Need to Know About Google Buying Fitbit*, OUTSIDE (Nov. 8, 2019), https://www.outsideonline.com/outdoor-gear/gear-news/google-bought-fitbit-heres-what-you-need-know/ [https://perma.cc/X7W3-EBNJ] (reporting that Fitbit had twenty-eight million active users in late 2019).

2. *Fitbit Privacy Policy*, FITBIT, http://www.fitbit.com/global/us/legal/privacy-policy [https://perma.cc/3FK5-FU5J] (Sept. 16, 2022). Identical language appeared in the version of Fitbit's Privacy Policy in effect at the time of the Google acquisition. *Previous Privacy Policies*, FITBIT (Sept. 18, 2018), https://www.fitbit.com/us/legal/previous-terms/09182018 [https://perma.cc/38EK-KFCZ].

enforceability.[3] Most U.S. privacy regulation builds on that textual base, which allows firms to acquire, use, and share consumer information if the consumer consents to a set of platform terms. But while a growing chorus of scholars, policymakers, and consumer advocates have criticized platform terms for being overly complex and procedurally underhanded and for permitting large data transfers like Fitbit's transfer to Google without meaningful consumer consent, consumer privacy reform stumbles along at a glacial pace dictated by continuing adherence to the notice-and-consent paradigm, regularly operationalized via the law of contracts.[4]

This Article reframes the discussion by demonstrating the unsuitability of contract law and reasoning in governing the consumer-platform relationship. It draws on close analysis of hundreds of sets of platform terms and smartphone app update histories to show that platform terms, as contracts, are effectively illusory. Beyond the realm of contract, this Article demonstrates that any regulatory approach based on notice-and-consent is doomed to failure.

Nearly every website, app, and device demands that its users agree to the platform terms.[5] From the *New York Times* to Neopets, we encounter these textual hurdles constantly.[6] One study found that it would take hundreds of hours per year for the average American to read all of the privacy policies to which they are subject, at an estimated total national cost of $781 billion annually.[7] Another study found that the

---

3. *See, e.g.*, Shmuel I. Becher & Uri Benoliel, *Sneak in Contracts*, 55 GA. L. REV. 657, 688 (2021) (noting that courts typically enforce contracts of this type). In particular, contract law has settled on the view that terms of service are enforceable contracts. Although privacy policies on their own usually do not constitute contracts, they are routinely incorporated by reference into terms of service and treated as contracts by courts. *See infra* Section I.A.

4. For example, the widely heralded California Consumer Privacy Act continues to permit extensive data collection, use, and transfer if authorized by consumer consent. *See, e.g.*, CAL. CIV. CODE § 1798.121(b) (2020) ("A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information . . . shall be prohibited . . . from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction *unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes*.") (emphasis added).

5. The well-known and much reviled "clickwrap" contract is a common delivery method for platform terms. Clickwrap contracts are electronic contracts in which a consumer must click an "I agree" button or checkbox in order to proceed. *See, e.g.*, Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1175–76 (9th Cir. 2014) (defining "clickwrap" and "browsewrap" contracts and noting that clickwrap agreements are more readily enforceable). Scholars have long noted the consumer protection issues inherent in clickwrap and browsewrap contracts. *See, e.g.*, Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 464 (2006) (contending that browsewrap should only be enforced between "sophisticated commercial entities"); Margaret Jane Radin, Commentary, *Boilerplate Today: The Rise of Modularity and the Waning of Consent*, 104 MICH. L. REV. 1223, 1225 (2006) (noting that the rise of modular, boilerplate online contracts might "exacerbate the divide between haves and have-nots").

6. Both require agreement to their respective Terms of Use and Privacy Policy to create an account. *See Login or Create an Account*, N.Y. TIMES, https://myaccount.nytimes.com/auth/login [https://perma.cc/G3QH-FJBC]; *Sign Up*, NEOPETS, https://www.neopets.com/signup/index.phtml [https://perma.cc/3GE6-V5W6].

7. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & POL'Y FOR INFO. SOC'Y, 543, 563–65 (2008) (reporting range of

privacy policies of platforms like Airbnb, Hulu, and CNN exceeded Immanuel Kant's *Critique of Pure Reason* in measures of reading difficulty.[8]

For good reason, the sheer volume of platform terms has concerned scholars, policymakers, and consumer advocates alike. A robust literature in contract law, for example, has argued that the volume and complexity of platform terms renders them practically incomprehensible.[9] Contracts scholars have also shown that the platform terms fail to communicate firms' practices to consumers.[10] Similarly, robust literatures in privacy law and consumer protection uncover the underhanded ways that firms obtain consumer consent, such as using "dark patterns" to nudge consumers toward accepting terms without ever reading or understanding them.[11]

---

estimated time to read applicable privacy policies from 181 hours per year to 304 hours per year, with a point estimate of 244 hours per year, and estimated national cost range from $559.7 billion to $1.1 trillion, with a point estimate of $781 billion).

8. *See* Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html [https://perma.cc/6TJ9-CR34].

9. *See, e.g.*, Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Procedural Privacy Protections*, 57 COMMC'N ACM, Nov. 2014, at 31, 32 (discussing the "'*transparency paradox*': simplicity and fidelity cannot both be achieved because details necessary to convey properly the impact of the information practices in question would confound even sophisticated users, let alone the rest of us."); Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO., COMMC'N & SOC'Y 1, 12, 16 (2018) (reporting results of study in which only 1.7% of participants mentioned issues with a clause in a set of experimental platform terms that would require the consumer to "assign their first-born child" as payment for services); *see also* Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. LEGAL STUD. S41, S65–66 (2016) (reporting that simplifying disclosures does not increase consumer understanding).

10. *See, e.g.*, Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 665–72 (2011) (demonstrating that in contexts including boilerplate consumer contracts, mandated disclosure is not effective at achieving any of its regulatory goals); Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S87 (2016) (reporting results of study showing no difference in comprehension between platform terms that had been deemed legally insufficient compared to terms that had been found enforceable); Kenneth A. Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On & Irwin Reyes, *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKELEY TECH. L.J. 327, 347–51 (2020) (finding that premium versions of free apps generally displayed similarly intrusive privacy practices).

11. As an initial matter, many privacy scholars have noted the implications of individuals' bounded rationality in assessing privacy risks. *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1887 (2013) (discussing studies demonstrating "the falsity of the traditional rational agent model of human decisionmaking"); Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442, 477–78 (2016) (noting the influence of factors including "asymmetric information, bounded rationality, and various heuristics" and that "some individuals' privacy-sensitive decision making—even that of well-informed and privacy-sensitive subjects—may be affected by cognitive and behavioral biases"); Idris Adjerid,

While these critiques are valid and important, they cede the battleground to the platforms by focusing on the text of the terms. This Article seeks to shift the focus. Through a close analysis of platform terms, this Article shows that platform terms lack key characteristics of contracts and, in the language of contract law, ultimately prove illusory. Applying contract-like reasoning to a relationship governed by such documents fatally undermines existing privacy regulations—even those heralded as providing strong privacy protection—because to do so allows fictitious consent to bless the collection, use, and sharing of private information. Such regulations provide only the trappings of privacy protection.

At the heart of this Article is a close analysis of a large, hand-collected set of platform terms from major websites and a separate set of update histories of popular smartphone apps.[12] This analysis reveals that platform terms bear almost no resemblance to contracts. In particular, this Article highlights three major findings.

First, firms enjoy unconstrained power to change every aspect of their "contractual" relationship with consumers on a whim. Of the hundreds of sets of platform terms analyzed, all but one allow the firm to change the platform terms unilaterally without consumer consent. Indeed, many expressly provide that the firm need not even notify consumers of a binding change in the terms and place the burden on consumers to keep up with modifications.

Second, firms enjoy equally unconstrained power to change their software, services, and devices. The Facebook that exists today is meaningfully different from the service for which untold millions of consumers signed up; in the era of the Internet of Things, the same can be said of household devices, ranging from laundry machines to light bulbs.[13] Yet, just as with updates to platform terms, firms

---

Sonam Samat & Alessandro Acquisti, *A Query-Theory Perspective of Privacy Decision Making*, 45 J. LEGAL STUD. S97, S114 (2016) (reporting results of study showing that consumers exhibit "both rational and behavioral responses to privacy settings"). Platforms can and do exploit those cognitive biases to obtain consent in various ways. *See, e.g.*, Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO., COMMC'N & SOC'Y 118, 119 (2017) (discussing "hypernudging" as a technique by which firms use Big Data to "configur[e] and thereby personalis[e] the user's informational choice context"); *see also* Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites*, PROC. ACM HUM.-COMPUT. INTERACT., Nov. 2019 at 81, 81:25 (discussing the increasing use of "dark patterns" designed to induce consumer consent); Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 46–47 (2021) (reporting on results of study showing that dark patterns are highly effective).

12. As discussed in further detail below, these datasets include 122 unique sets of platform terms and update histories of 100 popular smartphone apps on Google's Play Store. *See infra* Sections II.A–B.

13. The differences enabled by modern technology are not all for the best. For example, in May 2020, one smart-home device company imposed a new subscription fee on its customers with only a week's notice; failure to pay the fee would result in customers' already purchased devices ceasing to function properly. Jay Peters, *Smart Home Platform Wink Will Require a Monthly Subscription Starting Next Week*, THE VERGE (May 6, 2020, 8:36 PM), https://www.theverge.com/2020/5/6/21249950/smart-home-platform-wink-monthly-subscription [https://perma.cc/E73Z-B8YH].

frequently fail to disclose what they are changing and why. Substantial practical and legal obstacles impede consumers' ability to understand these updates. Worse, the pressing need to keep up with security updates compels consumers—including those concerned about privacy—to accept these mysterious updates, which arrive with astonishing frequency. Some of those updates imperil individual privacy in ways that individuals are powerless to understand or resist.

Third, firms generally retain the right to transfer consumer information in the event of a merger or sale. These transactions are incredibly common and, indeed, represent the end goal of many a startup.[14] A given individual might reasonably believe that the proprietor of an interesting new app is serious when it says it cares about privacy. But that commitment is obviated when, inevitably, Google or another Big Tech company comes along to acquire that startup, data and all, as permitted by assignment provisions in the platform terms.[15] And even if these kinds of data-transfer provisions were omitted in the initial set of platform terms, it is all but certain that the initial set *did* include a unilateral modification provision that would allow the startup to contractually bless data transfers in advance of a sale.

This Article therefore demonstrates that platform terms are freely modifiable by firms, who offer services and devices that are also freely modifiable in ways that fundamentally change those products and may imperil consumer privacy, which gather information that those firms intend someday to transfer wholesale to larger entities. There is little, if any, constraint on firms' power in these areas. And yet consumers are typically bound by the platform terms—agreements with no set provisions, governing no set services, with a counterparty to be named later. To call such agreements contracts is to stretch the concept beyond meaning. But courts, sometimes reluctantly, enforce them as such, and fall back to a contract-law approach even when considering statutory claims that do not depend on the existence of a contract. Regulators, too, speak the language of contract in their infrequent privacy enforcement efforts.[16]

Attempts to regulate privacy by regulating platform terms are doomed to failure, precisely because they lead to application of contractual rules to noncontractual relationships that are not susceptible to real contractual arrangements. Meaningful privacy regulation must proceed from a different paradigm—direct regulation of firms' collection, use, and transfer of data.

This Article proceeds as follows. Part I sets the stage by providing an overview of existing scholarship about the consumer-platform relationship. Most of this scholarship cedes the premise that platform terms are worth fighting over, which limits any effective reform of the consumer-platform relationship. Part II shows that platform terms neither look nor behave like contracts, despite courts' and regulators' reliance on contract reasoning when evaluating privacy issues. It identifies numerous dynamics, such as the malleability of both terms and services—and even the entities in the relationship—that render contract reasoning inappropriate. Part III considers

---

14. *See, e.g.*, Becky Peterson, *Half of All Startups Expect to Get Acquired, but the Number of Companies That Don't have a Plan is Growing*, BUS. INSIDER (Feb. 23, 2019, 8:30 AM), https://www.businessinsider.com/silicon-valley-bank-survey-half-of-all-startups-expect-to-be-acquired-2019-2 [https://perma.cc/TB2V-3PL4].

15. *See infra* Section II.B.3.

16. *See infra* Section I.A.

the implications of these dynamics for privacy regulation. In particular, it argues that there cannot be any version of notice-and-consent-based regulation that provides real privacy protection. By understanding that the consumer-platform relationship escapes the boundaries of contract, this Article illuminates new, fruitful directions for consumer protection and privacy regulation.

I. THE LIMITS OF PLATFORM TERMS

Platform terms are everywhere. They gatekeep access to daily computing necessities like Google's and Microsoft's suites of services. Unfortunately, they are also the primary line of defense between a person's private information and how a platform can use it. In an increasingly digitized world, the amount and precision of that information only increases. Many people track their location, fitness, nutrition, and health online using devices and apps provided by firms like Apple, Fitbit, and Garmin. Recent graduates track and pay their student loans through online portals. Millions of people track their menstrual cycles with apps. Confidential communications with one's doctors or professors increasingly take place via smartphones and websites. All these activities are governed largely, if not exclusively, by platform terms.

Even though platform terms govern so many important aspects of daily life, they are very lightly regulated. Courts and regulators embrace the notion that, as a matter of contract law, these terms are binding contracts. Consumers, after all, affirmatively assent to the platform terms when signing up for an account. Most efforts at reform have focused on making terms more understandable to consumers.

This contract-centered view bleeds into privacy regulation. American privacy law embraces the view that privacy requirements are irrelevant if individuals have notice of how their data is being used and consent to that use.[17] In other words, when consenting adults willingly give their data away in exchange for access to a website, there is no place for further regulation. Thus, many scholars focus their critiques on the margins, working on issues such as the complexity of notice, its apparent ineffectiveness, and the exploitive ways in which consent is often obtained.[18]

While important and convincing, these critiques all center on the platform terms. In the later Parts, this Article shows that this focus is futile because, as far as privacy protection is concerned, there can be no suitable regulatory regime based on notice and consent.

This Part lays the groundwork by showing how contract law has infected privacy protection, from treatment in the courts to the focus of scholarly critique. Section I.A explores the contractual status afforded to platform terms in litigation and enforcement. Section I.B considers contract law critiques of platform terms. Much of this literature takes as given that platform terms are contracts, and its critiques of the regime are therefore largely practical in nature, focusing on adequacy and

17. This has been the dominant approach since the earliest official privacy guidelines in the United States, the 1973 Fair Information Practice Principles. *See, e.g.*, Solove, *supra* note 11, at 1882 ("[M]ost forms of data collection, use, and disclosure are permissible under the FIPPs if individuals have the ability to self-manage their privacy — that is, if they are notified and provide consent.").

18. *See infra* Sections I.B–C.

effectiveness of notice. Section I.C examines critiques from the privacy literature, including firms' exploitation of cognitive biases to influence consumer behavior, the massive power disparity between firms and consumers, and the inadequacy of the purely procedural protections created by the notice-and-consent regime.

A. Platform Terms as Contracts

The numerous failings of platform terms provide ample support for the argument that they should not be treated as contracts. But that battle is lost. Over the last thirty years, courts charted a course from shrinkwrap to clickwrap that generally deems terms of service enforceable contracts.[19] Privacy policies often come along for the ride. Even where contract law is not specifically at issue—for instance, when analyzing statutory claims subject to a defense of consent—contract law regularly comes to the fore. There is, after all, no free-floating law of notice and consent; courts and regulators look to contract law to fill the gap.

Moving much of modern life to the internet necessitated developing an approach to online contracting. That, in turn, led to the creation of both legal standards to guide courts in their interpretation of online contracts and various methods of contracting falling in and around those standards. Nancy Kim identifies "notice-and-manifestation" as the prevailing legal standard, arguing that "[c]ourts seem to have conflated the doctrinal rules applicable to different contract forms to conjure up the standard of 'reasonable notice' and 'manifestation of assent.'"[20] Guided by that standard, two primary methods of online contracting developed: clickwrap and browsewrap. Clickwrap—documents to which the consumer manifests assent by clicking a button labeled with some version of "I agree"—has prevailed, with courts tending to enforce such agreements.[21] Browsewrap agreements—in which the terms are available on a website but the consumer is never required to view them or manifest assent—have been subjected to significantly more scrutiny.[22] To be sure, attempts to use browsewrap agreements persist, but given the relative difficulty of enforcing them, they are less commonly encountered than clickwrap agreements.[23]

---

19. Subject, of course, to traditional contract defenses such as unconscionability.

20. Nancy S. Kim, *Ideology, Coercion, and the Proposed Restatement of the Law of Consumer Contracts*, 32 LOY. CONSUMER L. REV. 456, 467 (2020).

21. *See, e.g.*, Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 465–66 (2006) (defining "clickwrap" agreements); *id.* at 459 ("Every court to consider the issue has found 'clickwrap' licenses . . . enforceable"); Kim, *supra* note 20, at 471 ("The early cases tended to accept clickwraps as valid contract forms because the click indicated that the user had received notice, had an opportunity to read the terms, and had manifested assent to them."); Tompkins v. 23andMe, Inc., No. 5:13-CV-05682-LHK, 2014 WL 2903752, at *12 (N.D. Cal. June 25, 2014) (noting that "courts have tended to enforce" clickwrap contracts, but not browsewrap contracts).

22. *See, e.g.*, Lemley, *supra* note 21, at 460 (defining "browsewrap" agreements); Kim, *supra* note 20, at 471 (noting that, compared to clickwrap agreements, "[b]rowsewraps were more difficult to prove").

23. For instance, in *Tompkins*, Judge Koh noted that the DNA testing service 23andMe's terms of service constituted both browsewrap and clickwrap because the "website did not require customers to acknowledge the TOS during purchase" of a testing kit but did require clicking an "I ACCEPT" button to create an account or register their kit. In keeping with the

Privacy policies are a different, and much more controversial, story. A discussion draft of the Restatement of the Law of Consumer Contracts prompted vigorous debate that has lasted for years about whether a privacy policy is a contract.[24] It is certainly true that, in many cases, courts have found privacy policies, standing alone, do not constitute contracts.[25] But even if a privacy policy, standing alone, is not always a contract, that does not mean it cannot be part of a contract.[26] Firms routinely incorporate their privacy policies into their terms of service by reference, giving the policies contractual effect that they might lack on their own.[27]

---

general trend, the terms were therefore held to be unenforceable against consumers who purchased test kits but did not create an account or register a kit. *Tompkins*, 2014 WL 2903752 at *9–11.

24. *See, e.g.*, Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45 (2019) (criticizing Restatement authors' quantitative study of whether courts enforce privacy policies as contracts); *cf.* Adam J. Levitin, Nancy S. Kim, Christina L. Kunz, Peter Linzer, Patricia A. McCoy, Juliet M. Moringiello, Elizabeth A. Renuart & Lauren E. Willis, *The Faulty Foundation of the Draft Restatement of Consumer Contracts*, 36 YALE J. ON REGUL. 447 (2019) (criticizing Restatement authors' quantitative studies of enforceability of unilateral modification provisions and of clickwrap contracts); Kim, *supra* note 20 (criticizing certain proposed provisions of the Restatement as contrary to the state of consumer contract law and as unsound policy). It bears noting, however, that the basis of the critiques of the quantitative studies is that they do not sufficiently support the particular draft Restatement terms. *See, e.g.*, Klass, *supra* note 24, at 55–56 ("The significance of the proposed comment 9 is not its affirmation that consumers and businesses *can* contract over privacy, but what it says about *how* they can do so."). The results of both Klass's and Levitin et al.'s replication studies suggest differences of degree, not kind. *See id.* at 49 ("[W]hereas the Reporters find that courts are seven times more likely than not to recognize that a business's privacy policy might be part of its contract with the consumer, I find a ratio of less than three to one."); Levitin et al., *supra*, at 464 ("For the relevant cases in this dataset, our findings are directionally the same as those reported in the draft Restatement, yet our findings show that there is an existing significant minority position: courts are not uniform in enforcing clickwrap contracts as the draft Restatement mistakenly claims.").

25. *See, e.g.*, Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (dismissing breach of contract claim based on airline privacy policy in part because "broad statements of company policy do not generally give rise to contract claims"); *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 611 (9th Cir. 2020) (affirming dismissal of breach of contract claim based on Facebook's privacy policy because it "merely provides information—not commitments—regarding Facebook's use of information and how users can control that information"); *cf. In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1331–32 (N.D. Ga. 2019) (noting that "[c]ourts have concluded that a business's privacy policy can constitute a stand-alone contract," but that plaintiffs failed to prove a contract existed because they "have not explicitly alleged that they read the Privacy Policy, or otherwise relied upon or were aware of the representations and assurances in the Privacy Policy," and therefore "failed to establish the essential element of mutual assent").

26. *See, e.g.*, Klass, *supra* note 24, at 55 ("[T]he claim that a consumer contract can include provisions related to use of the consumer's data is uncontroversial. Contract law is largely content neutral . . . . One does not need an empirical study to show that parties can contract to expand or reduce one side's privilege to share information generated in the transaction.").

27. The vast majority of terms of service analyzed referred to an accompanying privacy policy—forty-seven sets of terms expressly incorporated the privacy policy, while sixty-two

The requirements of incorporation by reference vary across jurisdictions, but for present purposes, the law of California looms largest.[28] And California law, for better or worse, does not require much to incorporate a document by reference. As one court noted:

> California case law makes it quite easy to incorporate a document by reference. "The contract need not recite that it incorporates another document, so long as it guides the reader to the incorporated document." What's needed is simply that the reference to the document be unequivocal, that the document be called to the attention of the contracting parties, and that the terms of the document be easily available to the contracting parties.[29]

Thus, the court found that multiple references to the Facebook Data Use Policy in its operative terms of service, including a link to the policy at the end of the terms, sufficed to incorporate it by reference, despite the absence of any language stating that the consumer agreed to the policy.[30] Many platforms make the connection more explicit. For example, Twitter's sign-up page indicates that "[b]y signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use."[31] The first item in its terms of service states that "the Twitter User Agreement comprises these Terms of Service, our Privacy Policy, the Twitter Rules and Policies, and all incorporated policies."[32]

Other jurisdictions require more to incorporate a contract by reference. In New York, "[t]he standard for incorporation by reference is an 'exacting' one," requiring "that the paper to be incorporated into the written instrument by reference must be so described in the instrument that the paper may be identified beyond all reasonable doubt."[33] But that bar is far from insurmountable, and approaches like Twitter's would seem to satisfy it.

---

referred to it. Whether those references suffice to incorporate the privacy policy into the terms is text- and jurisdiction-specific.

28. A plurality of terms analyzed (forty-three sets) elected California law to govern their interpretation. New York law was the second-most frequently chosen (twenty-six sets); no other jurisdiction was chosen in more than seven sets of terms. Among the terms of service electing California law, seventeen expressly incorporate the privacy policy and twenty-four refer to it; only two of these firms' terms of service lacked a reference to the privacy policy.

29. *In re* Facebook, Inc. Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 791 (N.D. Cal. 2019) (citations omitted).

30. Throughout the opinion, the court recognized the farcical nature of treating platform terms as contracts, noting that it was "[c]onstrained by th[e] fiction" that consumers have read the terms of service. *Id.* at 789. The court further noted that, "[o]ne could argue that the California appellate courts have been too quick to find incorporation by reference and that more explicit language should be required, particularly in the context of consumer contracts of adhesion. But this Court must apply California case law, which militates in favor of the conclusion that the Data Use Policy is incorporated into the [terms of service]." *Id.* at 791.

31. TWITTER, https://twitter.com [https://perma.cc/4ZFK-T7F3].

32. *Twitter Terms of Service*, TWITTER, https://twitter.com/en/tos [https://perma.cc/4ZJB-CZF9].

33. Fero v. Excellus Health Plan, Inc., 502 F. Supp. 3d 724, 742–43 (W.D.N.Y. 2020)

Treating platform terms as contracts matters for more than just contract claims—it is frequently how courts operationalize notice-and-consent privacy protections. Application to contract claims is straightforward: plaintiffs can use platform terms as a sword to assert a breach of contract claim; defendants can use them as a shield in order to argue plaintiffs consented to whatever activity they are challenging. But courts apply the contractual approach even when analyzing noncontract claims because the notice-and-consent approach to privacy protection invites, if not requires, that approach. For example, in *Calhoun v. Google LLC*, plaintiffs brought suit alleging that Google's Chrome browser secretly sent personal information to Google, contrary to representations made in Google's platform terms.[34] Among other claims, plaintiffs alleged violations of the Wiretap Act and the Stored Communications Act. Google sought dismissal of the claim based on both statutes' consent exceptions, arguing that its privacy policy disclosed the challenged practices.[35] In setting forth the applicable standards, Judge Koh noted that "[i]f a reasonable user could have plausibly interpreted the contract language as not disclosing that the defendant would engage in particular conduct, then the defendant cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent)."[36] Judge Koh rejected Google's consent defense in part because Google's then-applicable Terms of Service "explicitly excluded Google's Privacy Policy" and therefore the privacy policy was not incorporated into the terms of service.[37] Not surprisingly, neither the Wiretap Act nor the Stored Communications Act requires a contract to establish the consent exception.[38] But in the context of platforms like Google and Facebook, any such consent can only realistically be manifested via platform terms. Courts afford those terms contractual status and employ contract law in analyzing them, whether in reference to a contract claim or not.

Little changes when the Federal Trade Commission (FTC) acts to protect individual privacy because it is against the contractual platform terms that violations are measured. For example, in 2021 the FTC settled its investigation of Flo Health,

---

(quoting Ward v. TheLadders.com, Inc., 3 F. Supp. 3d 151, 163 (S.D.N.Y. 2014)) (finding that breach of contract claims based on privacy policy allegedly incorporated by reference could not "be resolved on a classwide basis" because "there would need to be an inquiry into whether a given class member received a paper copy of the [agreement] or a link thereto, and, if he or she received a link, what language that link used").

34. 526 F. Supp. 3d 605, 614–15 (N.D. Cal. 2021).

35. *Id.* at 619.

36. *Id.* at 620 (alterations omitted) (quoting *In re* Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 789–90 (N.D. Cal. 2019)).

37. *Id.* at 621.

38. *See, e.g.*, Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. § 2511(3)(b)(ii) (providing that an "electronic communication service" provider may disclose contents of communications "with the lawful consent of the originator or any addressee or intended recipient of such communication"); Stored Communications Act, 18 U.S.C. §§ 2701(a)(1), (c)(2), 2702(b)(3) (permitting disclosure of communications "with the lawful consent of the originator or an addressee or intended recipient of such communication," and permitting access to "a facility through which an electronic communication service is provided" if "authorized . . . by a user of that service with respect to a communication of or intended for that user").

Inc. after it learned that Flo had "disclosed health data from millions of users of its Flo Period & Ovulation Tracker app to third parties."[39] The gravamen of the charge that Flo engaged in deceptive practices was that Flo disclosed that information in violation of its privacy policy without consumers' consent.[40] The FTC took Flo to task because it "repeatedly promised users that the Flo App would keep their health data private, and that Respondent would only use Flo App users' data to provide the Flo App's services."[41] Those "promises" were made in Flo's privacy policies.[42] Had the platform terms adequately disclosed Flo's conduct, the basis of the FTC's complaint would vanish. In terms of the nature of the claims asserted, the only difference between this type of government enforcement and a private civil action is the identity of the plaintiff. The essential inquiry is the same, whether styled as notice and consent or offer and acceptance. Nor is this a new phenomenon: Daniel Solove and Woodrow Hartzog long ago found that "[m]uch of the FTC's privacy jurisprudence is based upon a deception theory of broken promises. Some of these promises are explicit and clear, such as when a company violates its own privacy policy . . . ."[43] They also found "that one of the most important features of the FTC's deceptiveness jurisprudence deals with insufficient notice to consumers," and thus "vague language tucked away in dense boilerplate agreements might not always be an effective method of notice to consumers."[44] This issue—whether the platform terms sufficiently disclose the challenged practices to enable consumers to consent—requires resort to contractual interpretation whether by the FTC, as in the case of *Flo*, or by the courts, as in *Calhoun*, even though neither case actually dealt with a claim for breach of contract.

Thus, even when pressing or resolving noncontract claims, contractual interpretation is an inextricable part of regulators' and courts' approach to privacy issues. No wonder, then, that scholars continue to level criticism toward platform terms as contracts. Yet as long as notice and consent remains the controlling paradigm, consumers arguably benefit from application of contract law and reasoning. If a court treats contractual consent as dispositive on matters of privacy, individuals may invoke contract defenses such as unconscionability and breach of the implied covenant of good faith and fair dealing.[45] A free-floating approach to

---

39. *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of Their Health Data*, FED. TRADE COMM'N (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about [https://perma.cc/BUF8-XYHJ].

40. *See* Complaint ¶¶ 13–17, 51–56, *In re* Flo Health, Inc., FTC Docket No. C-4747 (June 22, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf [https://perma.cc/W5J5-AJTX].

41. *Id.* ¶ 13.

42. *Id.* ¶ 14.

43. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 628–29 (2014).

44. *Id.* at 634–35.

45. Granted, such defenses do not often meet with success. *See, e.g.*, Mark A. Lemley, *The Benefit of the Bargain* 10 (Stan. L. & Econ., Working Paper No. 575, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4184946 ("Courts rarely apply unconscionability, and doctrinal innovations have limited its reach.") (footnotes omitted).

consent could preclude resort to these defenses. Additionally, while claims for breach of contract may not be the most natural (or successful) avenue to protecting privacy, there are few other candidates in existing law.[46] And plaintiffs in high-profile privacy cases—like the Cambridge Analytica litigation—have enjoyed preliminary success seeking redress for privacy violations via claims for breach of contract.[47] Little to gain, perhaps, but nothing more to lose.

B. Contract Law Critiques

Perhaps the most frequent critique of platform terms is that they are impractical. They have been derided as unreadably long, and studies have shown that they typically use language that is difficult for the average person to comprehend. Moreover, it is hard for consumers to opt out of invasive data practices even when that option is made part of the contract, whether by its terms or by specific legal obligation. Given these shortcomings, it is no surprise that most consumers do not read platform terms at all—indeed, it is rational not to do so. The following subparts discuss some of the most prominent critiques of notice and consent based on the actual contractual text. While convincing, these critiques suffer the same flaw: by focusing on the text itself, they deal only with the initial state of the consumer-platform relationship, putting aside power disparities in the formation and, critically, the continuation of that relationship.

1. Textual Failings

Evaluating platform terms on their text and numerosity leads to the ineluctable conclusion that it is impossible for even the most diligent individual to engage meaningfully with them. The roots of these problems are both intuitive and pressing—it is difficult for many readers to parse the language of most platform terms and impossible for anyone to keep up with the sheer volume of notice.

Commentators have long argued that platform terms are too long, too complicated, and too numerous to be comprehensible. While such problems might seem to counsel in favor of simplifying platform terms, Omri Ben-Shahar and Adam

---

46. *See, e.g.*, Thomas D. Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193 (2020) (discussing high dismissal rate of privacy cases brought in federal court based on lack of standing in data-protection litigation since 2013); *id.* at 1227–29 (noting varying rates of courts finding standing in cases involving claims such as violation of state privacy statutes (sixty-two percent), federal privacy statutes (fifty-two percent), and non-tort common-law claims (fifty-one percent)).

47. *See In re* Facebook, Inc. Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 795–96 (N.D. Cal. 2019) (denying in part motion to dismiss claim for breach of contract). Plaintiffs in less fraught privacy actions have likewise asserted, to some success, claims for breach of contract. *See, e.g.*, *In re* Google Assistant Priv. Litig., 546 F. Supp. 3d 945, 964–68 (N.D. Cal. 2021) (denying motion to dismiss breach of contract claim on theories that Google violated its privacy policy "(1) by recording Plaintiffs' private conversations when they are not using their Google Assistant Enabled Devices; [and] (2) by disclosing to third parties Plaintiffs' private conversations without their consent").

Chilton found that to do so would not increase comprehension.[48] Their 2016 article tested internet users to see if two common forms of policy simplification—adherence to best practices and use of a warning label—would change user comprehension or affect behavior. They found no significant change in either case.[49] Even if policies could be simplified enough to be comprehensible, other scholars have noted that the simplification would likely come at the expense of providing adequate information to the reader.[50] In another study, participants were given either a short or long form and then questioned about its contents. Although recipients of the short form answered more of the questions than those who received the long form, neither group demonstrated understanding of key information that the form was intended to impart.[51]

Accordingly, confronted with a towering mass of unreadable text on an almost daily basis, most consumers, understandably, simply click "I agree" and move on with their lives. That choice seems to be both rational and the only practicable course. Jonathan Obar and Anne Oeldorf-Hirsch showed this empirically, studying hundreds of people's interactions with an experimental set of platform terms. They found that most participants simply ignored the privacy policy, and those who did read the policy tended to spend very little time on it—eighty-one percent of that group spent less than one minute reading the privacy policy, which, at 7977 words, would be expected to require twenty-nine to thirty-two minutes to read in its entirety.[52] Perhaps most startlingly, Obar and Oeldorf-Hirsh buried in their terms a clause in which users promised to "assign their first-born child" as payment for the services offered by the fictional platform.[53] Only 1.7% of participants mentioned issues with that clause.[54] Other studies have shown similar results.[55]

Generally, the "notice" component of notice and consent does not work. This failure is not unique to platform terms. Ben-Shahar and Schneider document the inadequacy of disclosure in a number of contexts, including truth-in-lending, informed consent to medical procedures, and contract boilerplate.[56] Among the

---

48. *See generally* Ben-Shahar & Chilton, *supra* note 9.

49. *See id.* at S65–66 (reporting results of effect of simplifying privacy policies).

50. *See* Barocas & Nissenbaum, *supra* note 9, at 32.

51. *See* NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 125 (2019) (citing Traci Mann, *Informed Consent for Psychological Research: Do Subjects Comprehend Consent Forms and Understand Their Legal Rights?*, 5 PSYCH. SCI. 140 (1994)).

52. *See* Obar & Oeldorf-Hirsch, *supra* note 9, at 16; *see also id.* at 13–16 (reporting that seventy-four percent of participants used a "quick-join clickwrap option" to accept the privacy policy without reading it, and those who did open the policy had a median reading time of 13.6 seconds).

53. *Id.* at 12.

54. *Id.* at 16.

55. Such studies include findings that 22,000 participants agreed to clean toilets in exchange for access to free Wi-Fi and that only one percent of consumers read terms of service. *See* Charlotte A. Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505, 1521–22 (2019) (collecting studies on consumer behavior regarding terms of service and privacy policies).

56. *See* Ben-Shahar & Schneider, *supra* note 10, at 665–72 (noting that "[t]he great paradox of the Disclosure Empire is that even as it grows, so also grows the evidence that mandated disclosure repeatedly fails to accomplish its ends" and cataloging disclosure regimes

reasons they identify for that failure are the complexity and quantity of disclosures to which people are subject.[57] Disclosers' control over the form of disclosure leads to obvious conflicts of interest. Particularly in the context of privacy, disclosure of a platform's practices of using and often selling consumer data might be expected to deter participation. It comes as no surprise that platforms have often been reticent to disclose that type of information. When forced to disclose, their second-best option is to make that disclosure as unhelpful as possible.[58]

Looking to the courts to police ineffective disclosure will not improve the situation. As an initial matter, courts confronted with privacy claims regularly dismiss lawsuits for lack of standing.[59] But when courts have issued merits rulings on the propriety of particular terms, they have created distinctions without a difference. Lior Strahilevitz and Matthew Kugler show that consumer perceptions of platform practices are the same whether the particular policy language was deemed legally sufficient or lacking.[60] That consumers in this study understood a legally ineffective disclosure to authorize intrusive data practices perhaps speaks to a widespread understanding that platforms will engage in such behaviors as frequently as possible.[61] Since the practices themselves have generally been found legal, why spend the time to read the notice? Conversely, what appears to constitute functional notice to a thoroughly briefed and capably advised judge will likely remain incomprehensible to the lay reader with better things to do than pore over the minutiae of a single set of platform terms for hours at a time.

Unless a competitive market for terms and practices exists, individuals face the choice between, for instance, letting Facebook do what it will with their data or not participating in one of the world's largest social networks. When the "opt-out" cost is so high, there is no reason for an individual to bother reading the documentation setting forth the terms of participation.[62] There is, unfortunately, no market for platform terms—platforms do not, and do not have to, compete with each other for consumers' business by offering more favorable contracts.

---

that have failed to achieve their stated ends).

57. *See id.* at 686–90 (describing the "'overload' effect and the 'accumulation' problem" with mandatory-disclosure regimes).

58. *See, e.g.*, *id.* at 700–01 (noting that "[d]isclosers can also overdisclose in order to exacerbate the overload of disclosees," attempt to "beautify disclosure language," and "obey the letter of a mandate but flout its spirit").

59. *See, e.g.*, Haley, *supra* note 46.

60. *See* Strahilevitz & Kugler, *supra* note 10, at S87 (reporting results of study showing that "users of e-mail and social networking sites appear to regard even highly ambiguous privacy policy language as authorizing controversial company practices that implicate their personal privacy").

61. *Cf. id.* at S87 (positing "that consumers had formed strong prior beliefs about the sort of privacy-related conduct that companies are permitted to engage in, and these prior beliefs inform their understanding about what they agree to when they use Gmail or Facebook without changing their privacy settings").

62. *See, e.g.*, Oren Bar-Gill & Omri Ben-Shahar, *Optimal Defaults in Consumer Markets*, 45 J. LEGAL STUD. S137, S144 (2016) (using an economic model to show that when opt-out costs exceed the benefits of opting out, "there is no value in becoming informed," and therefore "all consumers remain uninformed and stick with the default").

To consider this critique requires considering its antagonist: in a nutshell, the argument that the market will provide better and more granular outcomes than regulation.[63] In this theoretical world, Instagram and Snapchat, for instance, are good substitutes for each other, and consumers might choose to use one or the other because of differences in their platform terms. As a result, Instagram and Snapchat would compete for consumers based on their platform terms and would be incentivized to produce terms that are consumer friendly (or at least relatively fair to consumers). And even though consumers generally do not read platform terms, the presence of a *marginal* consumer who *does* do so can provide that benefit to similarly situated consumers. Like a lead plaintiff in a class action lawsuit, the marginal consumer of platform terms advocates for everyone—so most consumers need only follow the marginal consumer's lead, and platforms, fearful of the marginal consumer, will once again offer platform terms that are consumer friendly.[64]

The reality, of course, is that there is no incentive for firms to compete on this front. The primary growth tool for many, if not most, platforms is to leverage network effects.[65] As a platform becomes more popular, it both gains in name recognition and becomes more attractive to new users. At the same time, individuals generally are unable to appreciate the privacy risks associated with any given activity, if they even care about privacy to begin with.[66] For those individuals who do care about privacy, cognitive biases make it difficult to understand the privacy implications of their activities. For example, Ignacio Cofone and Adriana Robertson have studied the prevalence of a bias called "non-belief in the law of large numbers," a bias that makes it difficult for individuals to understand how much is revealed by disclosure of any given piece of information about them.[67] Accordingly, most platforms stand to gain little by seeking to compete on privacy. Any platform that does seek to compete by offering more privacy-protective terms and practices merely cuts itself off from potential sources of revenue in order to offer people something most of them believe they do not need or want.

---

63. *Cf.* Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87 (2001) (contending that privacy regulation will overburden firms and advocating for market-based solutions to privacy concerns).

64. In the general context of consumer protection, Yonathan Arbel and Roy Shapira have extolled the potential value of "nudniks," who may provide social value by avoiding collective action problems, although they note that Big Data might make it easier for firms to identify and neutralize nudniks. *See* Yonathan A. Arbel & Roy Shapira, *Theory of the Nudnik: The Future of Consumer Activism and What We Can Do to Stop It*, 73 VAND. L. REV. 929 (2020).

65. "Network effects" refers to the economic concept that, for certain goods, "purchasers find a good more valuable as additional purchasers buy the same good." Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 483 (1998).

66. A surprisingly large number of people do not, it seems, care about privacy. *See, e.g.*, Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2026 (2013) (noting that approximately twenty percent of the population is "privacy unconcerned," meaning they are individuals "not valuing their own privacy and having a difficult time understanding why anyone would care about privacy").

67. Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1475 (2018) (describing the phenomenon of nonbelief in the law of large numbers and its relationship to information overload).

The empirical evidence bears out this line of reasoning. Reidenberg et al. have shown that the free market tends to produce vaguer privacy policies than those governed by some form of regulation.[68] Moreover, Marotta-Wurgler finds that while the content and protectiveness of privacy policies vary in predictable ways *across* markets, they do not vary *within* markets.[69] Both findings suggest that market forces do not provide options for privacy-minded individuals.

2. The Myth of the Perfect Notice

Considering these critiques, imagine the characteristics of the perfect platform terms. They would communicate enough information about the platform's business and technical practices to enable the reader to make an informed judgment about the risk of entrusting private data to the platform. They would also be comprehensible to the typical reader. When these two requirements are met, notice could theoretically be effective, allowing for at least the possibility of fairness in the initial relationship between consumer and platform. But these two requirements are mutually exclusive.

Barocas and Nissenbaum, for example, rightly argue that technical and legal complexity combine to preclude ideal platform terms. They dub this phenomenon the "*transparency paradox*: simplicity and fidelity cannot both be achieved because details necessary to convey properly the impact of the information practices in question would confound even sophisticated users, let alone the rest of us."[70] Examples abound. Consider a consumer interested in cloud-based backup services. A reputable provider would make available to the consumer sufficient technical information about its security practices to give that consumer comfort that their private information will not be mishandled. But understanding that information is no small feat, requiring a dizzying array of specialized knowledge just to have a handle on what the terms refer to, much less what they actually mean.[71]

---

68. *See, e.g.*, Joel R. Reidenberg, Jaspreet Bhatia, Travis D. Breaux & Thomas B. Norton, *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUD. S163, S182 (2016) (reporting results of study that "comparisons with the benchmarks indicate that the market produces privacy policies that are more ambiguous than those subject to some form of regulation").

69. *See, e.g.*, Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J. LEGAL STUD. S13, S31–33 (2016) (finding that, for instance, adult sites and cloud-computing sites tended to offer stronger privacy protection than social networks and gaming sites); *id.* at S35 (finding that "patterns [within markets] speak less directly to competitive outcomes"); *see also* Florencia Marotta-Wurgler, *Understanding Privacy Policies: Content, Self-Regulation, and Markets* 28 (N.Y.U. L. & Econ., Working Paper No. 16-18, 2016) (finding "relatively few significant differences" between privacy policies in the same market and noting "only scattered relationships between compliance measures and public versus private status, paid versus unpaid products, and site popularity").

70. Barocas & Nissenbaum, *supra* note 9, at 32 (endnote omitted).

71. As an example, the cloud-backup provider Backblaze provides extensive information about its security practices. The typical consumer likely will lack the baseline technical knowledge to understand the terms bandied about, such as the practice of putting passwords "through a hash and salt," and that data transfers involve encryption with "2048 bit public/private keys secur[ing] a symmetric AES-128 key." *Backblaze Security*, BACKBLAZE, https://www.backblaze.com/security.html [https://perma.cc/42NP-8CST].

For consumers who do not care about the technical details, legal complexity still stands in the way of comprehension. Meta (formerly Facebook) provides a striking example. For all the ink that is spilled about "terms of service" and "privacy policies," one might forgive a typical consumer for thinking that these two documents represent the entirety of any "agreement" they might have with a platform like Meta. Would that it were so simple. In fact, the "Terms of Service" adopted by Meta on January 4, 2022, incorporate by reference *twelve* "[o]ther terms and policies that may apply to you."[72] Notably, that list of possibly applicable terms and policies does not include either the "Cookies Policy" or "Data Policy," the latter of which is Meta's general privacy policy and, presumably, of significant importance to the privacy-minded consumer.[73] Untangling this mess of interweaving documents, some of which appear to have no legal effect,[74] would be no small undertaking even for a seasoned attorney. And, of course, no legal document would be complete without an array of defined terms, the definitions of which may confound the reader on their own with nested definitions and all manner of jargon.[75] In short, even evaluated purely through the lens of contract, Meta's platform terms are a mess.

---

72. Namely, the "Community Standards," "Commercial Terms," "Advertising Policies," "Self-Serve Ad Terms," "Facebook Pages, Groups and Events Policy," "Meta Platform Policy," "Developer Payment Terms," "Community Payment Terms," "Commerce Policies," "Meta Brand Resources," "Music Guidelines," and "Live Policies." *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/N5WC-7494] (July 26, 2022).

73. *See id.*

74. The Meta Brand Resources, for example, exhort the viewer to "[o]nly use the 'f' logo to promote your presence on Facebook. Don't use the Facebook wordmark, which is the corporate identity that refers to Facebook company." *Brand Overview*, FACEBOOK, https://www.facebook.com/brand/resources/facebookapp/guidelines [https://perma.cc/JNA5-NZHD]. Whether this term is meant to constitute a legal obligation is left as an exercise for the reader.

75. For example, the preamble to Meta's Terms of Service states that the terms apply to use of the "Meta Products," a term separately defined at great length: "The Meta Products include: Facebook (including the Facebook mobile app and in-app browser); Meta View; Messenger; Instagram (including apps like Boomerang); Meta Portal-branded devices; Meta Platforms Technologies Products such as Meta Horizon Worlds or Meta Quest (when using a Facebook or Meta account); Shops; Meta Spark; Meta Audience Network; NPE Team apps; Meta Business Tools; [and] Any other features, apps, technologies, software, or services offered by Meta Platforms, Inc. or Meta Platforms Ireland Limited under our Privacy Policy." *What Are the Meta Products?*, FACEBOOK, https://www.facebook.com/help/1561485474074139 [https://perma.cc/GR35-VEN3]. It specifically does *not* "include some Meta-offered products or services that have their own separate privacy policies and terms of service, like Workplace, Free Basics, Messenger Kids, Viewpoints, and Oculus Products when using an Oculus account." *Id.* That definition is not complete; it incorporates numerous other separately defined terms, including Facebook's entire "Privacy Policy" and the "Meta Business Tools," the definition of which links out to whole pages relating to "Meta Pixel," "Conversions API," "App Events via Facebook SDK," "Offline Conversions," and "App Events API," among others. *The Meta Business Tools*, FACEBOOK, https://www.facebook.com/help/331509497253087 [https://perma.cc/T73H-4EQX].

These technical and legal barriers to ideal notice affect both average and diligent consumers—even if one sat down to decode the voluminous notice that platforms provide, one might be led astray by the labyrinthine nature of nesting and cross-referencing policies written in inscrutable technical language.

In sum, the dominant notice-and-consent regime faces numerous intractable obstacles: platform terms are too difficult and numerous to comprehend, consumers therefore rationally decide not to read them, and the market has failed to provide meaningful alternative terms or practices to a theoretically notified individual. There does not appear to be any realistic prospect for solving these problems.

Platform terms are, therefore, not just bad contracts for consumers: they are bad *contracts*. But this panoply of contractual critiques rests largely on the terms themselves. Narrowly focusing discussions about privacy reforms on the text of platform terms necessarily limits the potential scope of reforms in ways that doom those efforts to failure.

Here, too, examples abound. Even legislative efforts heralded by privacy advocates—such as the California Consumer Privacy Act[76]—continue to rely on notice and consent as their basic model, despite the insurmountable issues with the platform terms that implement the model. Beyond legislation, many critics of the notice-and-consent paradigm likewise cannot resist attempting to save it.[77] Martin, for example, calls for "[m]ore work . . . to identify the minimums of the terms of use across consumers to help firms navigate informal privacy norms."[78] Davis and Marotta-Wurgler acknowledge the potential of regulation but prefer what they see as the improved flexibility of contract.[79] Thus, they advocate for regulations establishing "minimal protections combined with the flexibility of contract."[80]

Procedural improvements have been proposed as a possible means of mitigating the problems with notice and consent. Strahilevitz and Kugler, upon finding that the ambiguity of privacy-policy language does not appear to matter to consumers, propose turning the interpretation of consumer contracts into "a question of fact rather than a question of law," relying on surveys of consumer understanding to determine what practices are authorized by a given privacy policy.[81] When faced with an ambiguity about whether a certain action is permissible under a set of

---

76. *See, e.g.*, *Privacy Groups Praise CA Legislators for Upholding Privacy Law Against Industry Pressure*, CONSUMER REPS. (Sept. 13, 2019), https://advocacy.consumerreports.org/press_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/ [https://perma.cc/33ZN-DPKP].

77. Others have decided that discretion is the better part of valor. *See, e.g.*, Ben-Shahar & Schneider, *supra* note 10, at 651 ("Our task is *not* to propose an alternative.").

78. Kirsten Martin, *Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online*, 45 J. LEGAL STUD. S191, S211 (2016).

79. *See* Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U. L. REV. 662, 704 (2019) (contending that "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").

80. *Id.*

81. *See* Strahilevitz & Kugler, *supra* note 10, at S88.

platform terms, courts would simply survey the general populace to see what the average consumer believes is permissible. While these procedural reforms might mitigate some of the difficulties arising from treating contract as the first-line approach to protecting privacy, they likely will not move the needle on privacy protection. That is because, as discussed in Part II, no set of terms can handle the true complexity of the consumer-platform relationship.

C. Privacy Law Critiques

Numerous privacy scholars have joined in critiquing the textual failings of platform terms. But the privacy literature further emphasizes ways in which the notice-and-consent paradigm infringes upon, and weaponizes, consumer privacy. Relatedly, many have considered the moral and philosophical problems created by the notice-and-consent paradigm writ large.

The preceding section demonstrated that it is rational for individuals not to bother reading terms of service. But rationality is only part of the puzzle: studies show that individuals' decision-making about privacy exhibits both rational and behavioral tendencies. Further, as noted by Solove, Yeung, and Acquisti et al., among others, numerous studies discredit the idea that humans are strictly rational actors.[82] As platforms amass ever more data about everyone and everything, they grow better able to motivate particular behaviors—a power they exploit ruthlessly, as Yeung has shown.[83]

Evidence continues to mount that platforms can and do influence individuals' privacy practices and behaviors.[84] Recent scholarship identifies the rise of "dark patterns"—deeply deceptive methods of influencing consumer consent to platform terms—among other goals, that are as widely used as they are effective.[85] Scholars

---

82. *See, e.g.*, Solove, *supra* note 11, at 1887 ("Studies by Professor Daniel Kahneman, Professor Amos Tversky, and others demonstrate the falsity of the traditional rational agent model of human decisionmaking, as people often decide based on heuristics and the way choices are framed."); *see also* Yeung, *supra* note 11, at 125 ("Empirical studies demonstrate that individuals' privacy behaviours are easily influenced through environmental cues, such as defaults, and the design of web environments owing to pervasive reliance on heuristics and social norms."); Acquisti et al., *supra* note 11, at 477–78 (discussing studies demonstrating the impact of cognitive and behavioral biases, as well as information asymmetries, on individual decisions involving privacy); Leah R. Fowler, Jim Hawkins & Jessica L. Roberts, *Uncertain Terms*, 97 NOTRE DAME L. REV. 1, 41 (2021) ("[P]eople are often not rational actors and will, as a result, make suboptimal decisions.").

83. *See, e.g.*, Yeung, *supra* note 11, at 119 (noting that firms, using Big Data, engage in "hypernudging" by "configuring and thereby personalising the user's informational choice context, typically through algorithmic analysis of data streams from multiple sources claiming to offer predictive insights concerning the habits, preferences and interests of targeted individuals").

84. *See, e.g.*, *id.* at 125 ("Empirical studies demonstrate that individuals' privacy behaviours are easily influenced through environmental cues, such as defaults, and the design of web environments owing to pervasive reliance on heuristics and social norms.").

85. One study defines dark patterns as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make." Mathur et al., *supra* note 11, at

have identified numerous types of dark patterns and grouped them into certain categories such as asymmetric presentation and outright deception.

Mathur et al. describe a particularly common type of asymmetric presentation: a website pop-up with a notice that the website uses "cookies" to track user behavior, followed by a large button to accept cookies and a much smaller opt-out button (if an opt-out is even presented on the same page, which is often not the case).[86] Deceptive dark patterns are also common, and perhaps more clearly insidious. Mathur et al. note, for example, that websites—including reputable online clothing retailers—often present an apparently limited-time discount, encouraging consumers to buy right away, in order to take advantage of the discount. The discount, however, is not limited in duration: it repeats every time a consumer refreshes a web page.[87] These practices often appear designed to exploit known cognitive biases.

Although only recently receiving attention in legal scholarship, dark patterns are widely used and frighteningly effective. Using an automated crawler, Mathur et al. found dark patterns in use on eleven percent of eleven thousand shopping websites examined, with more popular sites more frequently employing dark patterns.[88] In their study of the effectiveness of dark patterns, Luguri and Strahilevitz found that use of aggressive dark patterns nearly quadrupled the rate at which participants accepted a for-pay data protection and credit monitoring service.[89] Worse, dark patterns proved more effective among participants with lower levels of education.[90]

Thus, it is not enough for platforms to reap the benefits of contract-adjacent privacy regulation that inherently disadvantages consumers. Platforms leverage cognitive biases and reams of personal information in their possession to wring ever more advantage out of the consumer-platform relationship.

This line of critique, too, ultimately leads to an argument about platform terms as contracts. Exploiting an individual's cognitive biases in order to get them to agree to an unfavorable contract arguably vitiates consent to that contract. But regulating platforms' ability to exploit biases for that purpose merely invites retrenchment to marginally fairer methods of obtaining consent. As the contract-focused critiques discussed above show, the market will not produce sufficiently protective terms, to say nothing of the unsolvable comprehension problem.

The practical and behavioral difficulties attending to consumer understanding and agreement to platform terms, coupled with firms' exploitation of cognitive biases and troves of data, discredit the notion that consumers have consented to anything. These difficulties implicate the underlying moral and philosophical basis for the

---

81:2. Jamie Luguri and Lior Strahilevitz situate dark patterns as examples of "sludge" and market manipulation, and generally define the term to mean "user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions." Luguri & Strahilevitz, *supra* note 11, at 44.

86. Mathur et al., *supra* note 11, at 81:5.

87. *Id.*

88. They note that this number represents a "lower-bound estimate of the prevalence of dark patterns" due to the crawler's limited capabilities. *See id.* at 81:11–81:12, 81:27.

89. Luguri & Strahilevitz, *supra* note 11, at 64.

90. *Id.* at 80; *see also id.* at 81 ("To summarize the data we have collected and analyzed here, it appears that several frequently employed dark patterns can be very effective in prompting consumers to select terms that substantially benefit firms.").

notice-and-consent regime—a line of critique that begins, at last, to gesture at notice-and-consent's total unsuitability for the purpose of governing privacy.

Considering the issue generally, Kim notes that a host of factors bear on individuals' decision-making, a fact that complicates the question of consent in all cases.[91] Of particular relevance to platform terms, Kim identifies the "important issue" of "whether consent to one activity includes consent to a progressive or more involved version of that activity, or whether another communicative act is required," which Kim argues should "affect[] the burden between the parties."[92]

Focusing on the consumer side of the consumer-platform relationship, Bietti identifies both the transformative role of consent and the reasons that, in the context of the platform economy, it should not be considered effective. In order to be "morally transformative," she contends that consent must concern a subject that is "capable of being transformed and not inalienable," "must not significantly harm third parties," and must be given free of unfair power disparities or other coercive conditions.[93] The typical platform obviously does not meet this third condition, as is apparent from the significant practical and cognitive impediments to meaningful consent.[94] Indeed, platforms appear to exploit market dominance and dark patterns to deprive individuals of any choice they might have had.

But the consumer-platform relationship also fails to satisfy the first two conditions identified by Bietti. As to alienability, interests such as being free from behaviorally targeted "undue political influence" should be considered inalienable.[95] Although certain self-interested parties might quarrel with that view, it seems uncontroversial that individuals should be free of such influences in exercising the right to vote.[96] Negative effects on third parties are also present in the platform economy. As one direct example, anyone is free to take photographs of people in

---

91. *See* KIM, *supra* note 51, at 3 ("Decision-making does not occur in a vacuum, but is affected by what the consenting party knows, the available options and the consenting party's emotional state at the time consent is granted. It is also affected by the actions of the party seeking consent. Accordingly, while the requirement of consent recognizes the value of autonomous decision-making, the *validity* of consent hinges upon the context in which it is given and the dynamic unleashed by both parties."); *see also id.* at 11–15 (collecting social science research on impediments to rational decision-making).

92. *Id.* at 8.

93. Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 310, 326 (2019) (arguing that "consent has no value if it is shaped by systemic and invisible exercises of power" and contrasting "morally transformative" consent against "idealized" consent, the latter of which is more typical in the platform context); *see also id.* at 365 ("[W]e must seriously question whether the emphasis on individualized notice and consent as a device which enables access and choice is appropriate and whether even the most extensive disclosure and the most freely given consent is actually sufficient to protect us from diffuse and systemic harms in the platform economy.").

94. *See, e.g.*, *id.* at 382 ("The problem is not only that individuals have no valid alternatives, or are unable to choose, or lack voluntariness or understanding, but also that consent is being weaponized by powerful industry actors to forward their agenda.").

95. *Id.* at 325.

96. *See, e.g.*, Fed. Election Comm'n v. Akin, 524 U.S. 11, 24–25 (1998) (holding that an "information injury . . . directly related to voting, the most basic of political rights, is sufficiently concrete and specific such that" it may be "vindicat[ed] in the federal courts").

public and upload those photographs to platforms. Other firms can then scrape those photographs for purposes including training facial-recognition systems and creating surveillance services with the results. Those systems have proven popular with police forces and authoritarian regimes, among others. Existing privacy regulation is the product of a time before regulators could even have conceived of such troubling, large-scale activity. Firms have moved faster than regulators, leading to the dystopian headlines that emerge on a regular basis.[97]

Even sharing information only about oneself negatively impacts third parties, as aggregation of self-disclosures can be used to infer information about similarly situated third parties.[98] Employing game theory, Yoan Hermstrüwer shows that, in today's platform economy, the only rational choice is therefore to disclose information.[99] While not as viscerally horrifying as the implications of massive databases of images, even such limited sharing fails to satisfy the conditions necessary to provide a moral basis for consent.

Legislative reforms, meanwhile, fail to address privacy scholars' critiques just as they do on matters of contract. The California Consumer Privacy Act has been hailed as one of the most protective of consumers.[100] But in addition to reifying the notice-and-consent paradigm, it does not even require consent to certain practices. Rather, it provides for an "opt-out" right that allows consumers to instruct business not to sell personal information about the consumer to "third parties"—an approach left substantially unchanged by the follow-up California Privacy Rights Act.[101] But given the widespread use of dark patterns, the feasibility of such a system seems dubious: as previously discussed, firms are notorious for making opt-outs extremely difficult to find and complete.[102]

---

97. *See, e.g.*, Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/G3VX-BHSH] (reporting on the company Clearview AI, which obtained a database of approximately three billion images from which it created facial recognition software that it licenses out to law enforcement and private entities).

98. *See, e.g.*, Barocas & Nissenbaum, *supra* note 9, at 32 ("The willingness of a few individuals to disclose information about themselves may implicate others who happen to share the more easily observable traits that correlate with the traits disclosed.").

99. Yoan Hermstrüwer, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data*, 8 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 9, 13 (2017) (showing that "[t]he refusal of consent is a dominated strategy that rational users will have no incentive to choose whatsoever").

100. *See Privacy Groups Praise CA Legislators for Upholding Privacy Law Against Industry Pressure, supra* note 76.

101. CAL. CIV. CODE § 1798.120(a) (2020). The revisions to this provision contemplated by the California Privacy Rights Act add data sharing to the list of activities subject to the opt-out right but do not otherwise curtail the opt-out. *See* CAL. CIV. CODE § 1798.120 (2020) as amended by Ballot Initiative 24.

102. *See, e.g.*, Hana Habib & Lorrie Cranor, *It's Shockingly Difficult to Escape the Web's Most Pervasive Dark Patterns*, FAST CO. (Nov. 4, 2019), https://www.fastcompany.com/90425350/its-shockingly-difficult-to-escape-the-webs-most-pervasive-dark-patterns [https://perma.cc/GCU7-VN2H] (noting various problems with opt-outs, including lack of standardized language, broken links, and unclear options).

Notice and consent have long served as the prevailing paradigm for privacy protection. The preceding subparts discussed critiques of the "terms" of platform terms—in short, they are bad contracts, and consumer consent to them is obtained via questionable means. But these critiques are of limited force because they engage primarily with the terms themselves, suggesting the possibility that refinement of terms could yield adequate privacy protection. In the following Part, this Article demonstrates numerous factors precluding any such result.

II. BEYOND THE INITIAL STATE

Part I of this Article focused on the limits of existing critiques of the notice and consent terms, all of which coalesce around platform terms as the primary form of regulation. But the consumer-platform relationship is much more complicated than existing accounts posit, foreclosing the possibility that any version of notice and consent might prove workable.

This Part shows that appropriate regulation of the consumer-platform relationship cannot be reduced to an ex ante writing. It relies on analysis of over one hundred sets of platform terms, as well as the update histories of one hundred popular smartphone apps, to make that case. While this Article is certainly not the first to analyze platform terms, this dataset has several unique features. First, it includes several important provisions not previously closely analyzed, including the prevalence of provisions allowing firms to transfer consumer data in the event of a merger or acquisition—provisions that severely undercut the supposed contractual nature of the consumer-platform relationship. Second, it includes update histories for smartphone apps, the frequency and opacity of which are critical to exploring an issue under-examined in the literature: firms can and do change the products and services offered to consumers without notice or any explanation of what they have changed.

The findings that emerge from close analysis of platform terms and app update histories show that platforms can and do unilaterally reshape their relationship with consumers after the time of contracting. Ultimately, when platforms enjoy unilateral control over what they offer and on what terms, contractual limitations cannot keep up. Familiar guardrails of contract law vanish: notice is effectively nonexistent and consent is an illusion.

To demonstrate the unsuitability of platform terms, this Part proceeds as follows. Section II.A begins with a brief note on methodology. Section II.B presents three major findings. First, firms almost universally reserve the right to change the terms on which they offer products and services at any time, frequently without notice. Second, platforms can and do change the products and services in ways that put individual privacy at risk. Third, firms regularly reserve the right to sell themselves—and all the consumer data in their possession—to entities with potentially inferior privacy practices, with individuals left unable to object.

A. Methodology

This Article presents findings from two original datasets collected in 2020 and 2021. The first set concerns platform terms. To create this dataset, a research assistant and I systematically analyzed and coded the platform terms of 145 websites, drawn from the top 150 websites on the English-speaking internet as listed by the

Alexa Top Sites service on November 27, 2020.[103] Common ownership of several sites led to duplication of terms—for example, Microsoft operates several of the top sites under the same set of platform terms—and duplicate sets of terms were excluded from analysis. Additionally, some of the top sites were operated by government-owned entities such as the United States Postal Service and were excluded. Finally, several websites in the top 150 did not appear to have platform terms available in English and were excluded. In all, 122 unique sets of terms of service and accompanying privacy policies (where present) were analyzed. Analysis was conducted on the platform terms available on these websites in December 2020 and January 2021.

For each set of platform terms, we recorded the date on which we accessed and analyzed the terms and the effective date of the terms (where stated). We then coded each set of terms on several issues, including:

- Whether the terms included a unilateral modification provision;
- The method, if stated, by which the platform would provide notice of a change in terms;
- Whether the terms included provisions authorizing the relevant entity to transfer consumer data in the event of an acquisition or other business combination;
- The governing law specified in the terms; and
- Whether the terms included (a) an arbitration clause, (b) a class-action waiver, or (c) a forum-selection clause.

The second dataset concerns smartphone app updates. To create the bulk of this dataset, in September 2021, a research assistant and I sourced and analyzed update information for the one hundred most popular apps on Google's Play Store at that time. For each app, we recorded the date and version number of app updates provided by AppBrain, a service that tracks information about apps on the Play Store.[104] Previously, in March 2021, we recorded the month and year of each update to the twenty most popular apps on Apple's App Store at that time,[105] as well as the patch notes accompanying each update. The App Store lists only the most recent twenty-five updates and accompanying patch notes for any given app; Google's Play Store does not require app developers to display patch notes and does not directly make historical update information available.

B. Findings

Analysis of these platform terms and update histories helps shed light on three major issues that complicate the consumer-platform relationship beyond contract's

---

103. *See* Becher & Benoliel, *supra* note 3, at 673 (noting that "[t]he Alexa Top Sites service is a leading website traffic measurement tool based on millions of internet users" and "is built on a significant sample of internet users [and is therefore] widely used as a source of data for empirical research") (footnotes omitted). Five of the top 150 listed were pornographic in nature and excluded from analysis.

104. *See* APPBRAIN, https://www.appbrain.com [https://perma.cc/HD2K-AD78] ("AppBrain App Intelligence provides detailed information about all apps on Google Play.").

105. Apple's App Store only displays, in months, how long ago a particular update was released.

ability to provide effective regulation. First, platform terms almost uniformly include provisions giving firms the right to unilaterally modify the platform terms, often without providing any notice to consumers. Second, firms routinely update the services and devices they provide, again without providing effective notice to consumers of what they are changing and why. Third, firms regularly reserve the right to transfer personal information to an acquirer in the event of an acquisition or similar business combination. By more fully exploring the complexity of the consumer-platform relationship, the unsuitability of notice and consent is laid bare.

1. Changing Terms

Most critiques of notice and consent focus on the terms offered and the relationship of the parties at the time of initial contracting—that is, the point at which a consumer signs up for a service, or first accesses a site with browsewrap platform terms. While there is much to say about what happens in that moment, this approach fails to grapple with the magnitude of what happens next.

The platform terms that govern the ongoing relationship between consumer and platform are dynamic. This is perhaps inevitable: for reasons both endogenous (e.g., deployment of a new feature) and exogenous (e.g., enactment of new regulations like the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act), the terms on which platforms are willing or able to offer their services change over time. Acquiring consent all over again whenever the platforms feel the need to change terms could prove complicated, to say the least.

Platforms deploy a simple solution to that problem: they include in the initial terms the consumer's agreement that the platform may unilaterally change the platform terms. Analysis of the 122 top websites reveals that every one includes in its platform terms a unilateral modification provision. These provisions are usually buried in long preambles[106] or paragraphs of "additional" or "miscellaneous" terms.[107] The method of acceptance is subject to only slight variation: consumers either accept the terms by continued use of the service[108] or the firm simply reserves the right to make changes.[109] Only *one* of the 122 websites analyzed did not include

---

106. *See, e.g.*, *Terms and Conditions*, BEST BUY (Apr. 29, 2022), https://www.bestbuy.com/site/help-topics/terms-and-conditions/pcmcat204400050067.c?id=pcmcat204400050067 [https://perma.cc/8UTJ-UVN9] (including unilateral modification provision in the seventh of nine sentences).

107. *See, e.g.*, *Terms of Service*, FACEBOOK (July 26, 2022), https://www.facebook.com/terms.php [https://perma.cc/WTJ4-VCQP] (including unilateral modification provision in section titled "Additional provisions"); *Terms of Service*, NETFLIX, https://help.netflix.com/legal/termsofuse [https://perma.cc/K8S6-9TD2] (Nov. 2, 2021) (including unilateral modification provision in section titled "Miscellaneous"); *see also Terms of Service*, GOOGLE, https://policies.google.com/terms?hl=en-US#toc-about [https://perma.cc/Y78Y-K3B9] (Jan. 5, 2022) (including unilateral modification provision in section titled "About these Terms").

108. *See, e.g.*, *Microsoft Services Agreement*, MICROSOFT (June 15, 2022), https://www.microsoft.com/en-us/servicesagreement [https://perma.cc/89KA-D7P3] (providing in section seven, that "[u]sing the Services after the changes become effective means you agree to the new terms").

109. *See, e.g.*, *Conditions of Use*, AMAZON (Sept. 14, 2022),

a unilateral modification provision in its terms of service: the privacy-focused search engine DuckDuckGo, which does not have any terms of service and has a privacy policy proclaiming that "DuckDuckGo does not collect or share personal information."[110]

Platforms also disclaim any obligation to inform their users of changes to terms. Among the 122 unique sets of platform terms analyzed, fifty-five expressly provide that they will do nothing more than post new terms of service to their websites.[111] Some platforms go further by purporting to place the burden to keep track of changes on the consumer.[112] The other approaches taken by leading platforms still leave much to be desired. Among those that make some commitment to notify consumers, many are notably vague about how they will do so; that is, they do not state whether notice will come via email, message on the platform itself, or some other means.[113] Twenty platforms pledge to provide notice only when changes to the terms are "material," with no explanation of what would constitute a material modification,[114] and often paired with the lack of commitment to any particular form of notice.[115] As noted above, none pledges to explain what the changes are, and in at least one case a platform has gone backward in this respect.[116] As a result, the generic commitment

---

https://www.amazon.com/gp/help/customer/display.html?nodeId=508088 ("We reserve the right to make changes to our site, policies, Service Terms, and these Conditions of Use at any time.").

110. Alas, DuckDuckGo was only the sixty-seventh most popular website at the time of analysis, falling well behind other search engines such as Google, Yahoo, and Bing. Moreover, DuckDuckGo implies that it retains the unilateral right to modify its privacy policy, although it pledges to provide some notice of such changes. *See DuckDuckGo Privacy*, DUCKDUCKGO (Apr. 11, 2012), https://duckduckgo.com/privacy [https://perma.cc/TDJ6-R6U3] ("If this policy is substantively updated, we will update the text of this page and provide notice to you at https://duckduckgo.com/about [https://perma.cc/H5RS-TQLW] by writing '(Updated)' in red next to the link to this page (in the footer) for a period of at least 30 days.").

111. *See, e.g.*, *Reddit User Agreement*, REDDIT (Aug. 12, 2021), https://www.redditinc.com/policies/user-agreement ("We may make changes to these Terms from time to time. If we make changes, we will post the revised Terms and update the Effective Date above.").

112. *See, e.g.*, *Disney Terms of Service*, THE WALT DISNEY COMPANY (June 9, 2020), https://disneytermsofuse.com/english/ [https://perma.cc/ADD9-T64H] ("You are responsible for periodically reviewing this Agreement for updates and amendments.").

113. *See, e.g.*, FACEBOOK, *supra* note 107, at § 4(1) ("[W]e will notify you before we make changes to these Terms and give you an opportunity to review them before they go into effect.").

114. *See, e.g.*, *Yahoo Terms of Service*, YAHOO (May 26, 2022), https://legal.yahoo.com/us/en/yahoo/terms/otos/index.html [https://perma.cc/4X2R-R55A] (providing in section twelve that Yahoo "will provide notice (in accordance with Section 3(c) above [of the Yahoo Terms of Service]) of material modifications").

115. *See, e.g.*, *Zillow Terms of Use*, ZILLOW GROUP (Sept. 23, 2022), https://www.zillowgroup.com/terms-of-use/ [https://perma.cc/5ASD-R7VL] (providing in section twelve that Zillow "will make commercially reasonable efforts to notify you of any material changes to these Terms of Use").

116. LinkedIn's May 8, 2018, user agreement update included a "summary of changes." The current user agreement, effective February 1, 2022, not only includes no such summary of changes, but there also does not appear to be any way to access previous versions of the

to notify consumers of changes does little to assist consumer comprehension of the new terms that govern their relationship with the platform.[117]

The reservation of a unilateral right to modify platform terms, coupled with refusal to commit to notifying consumers of changes, leads to modified terms that fall short of browsewrap in their capacity to provide meaningful opportunity for consumer understanding and agreement. In effect, consumers are generally left to do as the burden-shifting terms would require: constantly check platforms' legal pages for updates to the platform terms and carefully analyze them for changes. As though that did not already constitute an insurmountable task, websites typically do not provide access to prior versions of their platform terms. Short of maintaining a web crawler to constantly download the terms of every platform one uses and employing text-analysis software to determine if there have been any changes, it is difficult to envision how a consumer might keep track of what changes they have "consented" to over time.[118]

Unilateral modification provisions, on their own, fatally undermine the notice and consent approach to privacy regulation. Unnoticed changes to platform terms move the task of comprehending on what terms a consumer engages (or has engaged) with a platform from extremely difficult to impossible. This is particularly so given that many platforms expressly provide that changes to the terms of service do not have retroactive effect.[119]

Consider, for example, a person who has used Facebook since January 2005.[120] Suppose that user has posted, on average, once a week since joining. By the end of

---

agreement on LinkedIn's website. *See User Agreement*, LINKEDIN (Feb. 1, 2022), https://www.linkedin.com/legal/user-agreement [https://perma.cc/PE3Q-XKHK]. Indeed, the May 8, 2018, Summary of Changes, which was available at least as late as January 5, 2021, at https://www.linkedin.com/legal/user-agreement-summary [https://perma.cc/Y8QM-MHXA], is no longer available as of January 7, 2022.

117. In their recent study, Becher and Benoliel find that these problems extend further down the web as well. Surveying 500 websites popular in the United States, they found that 479 included a unilateral modification provision in their platform terms. Among those, 450 did not require the firm to notify consumers of changes individually; 454 did not require the firm to notify consumers as a class; and 141 expressly shifted the burden to the consumer to keep track of changes. Only one pledged to individually inform consumers of the substance of any change to the platform terms and did so ineffectively. *See* Becher & Benoliel, *supra* note 3, at 681–84. Likewise, Fowler, Hawkins, and Roberts find that "[u]nilateral amendment clauses are ubiquitous" in health apps. *See* Fowler et al., *supra* note 82, at 22–25.

118. The market appears not to have provided such a service, although one would certainly be useful. One effort at doing so, Docracy, last received an update in November 2013. *Docracy Terms of Service Tracker*, DOCRACY (Nov. 20, 2013), https://www.docracy.com/tos/changes [https://perma.cc/ATY5-EH9U]. Another, which has the backing of the Electronic Frontier Foundation, appears to have been rolled into the "Terms of Service; Didn't Read" project. *See* TOSBACK, https://tosback.org [https://perma.cc/SP2S-YJ8E]. While that project has the laudable goal of crowd-sourcing analysis and grading of platform terms, it does not appear to provide historical platform terms. *See* TERMS OF SERVICE; DIDN'T READ, https://tosdr.org [https://perma.cc/K2F9-2GH6].

119. *See, e.g.*, *Google Terms of Service*, *supra* note 111 (providing that "[c]hanges will not apply retroactively").

120. To the best of my recollection, that is when I joined Facebook.

2021, that person would have posted nearly 900 times. Suppose further that, in January 2022, that person wanted to understand the terms governing their many Facebook posts over the years. Not only would that person have to obtain copies of every version of Facebook's, and later Meta's, platform terms over that period—information that Meta does not make available—they would be forced to compare every version and match it up with whatever posts were made during each period. This is not achievable for any conceivable Facebook user. Indeed, it would appear that only a person with access to internal Meta documents, whether because they are an employee or obtained access via litigation, could even obtain the necessary platform terms to attempt the analysis.

Consider further the complex legal ramifications of unilateral modification provisions. Although wording varies, it is common for such provisions to state that a user who does not consent to a change in the terms of service must delete all of their information stored with the platform in order to "reject" the new terms.[121] Does such a provision negate any claim of nonretroactivity of new terms?[122] If a user manually deletes each of their Facebook posts but declines to close their account, have they effectively rejected the new terms? The answer to these questions is nonobvious even to an attorney; for the typical consumer, there is simply no way to know.

Unilateral modification also renders the choice to skip reading terms and conditions not only rational but inevitable. If it would take hundreds of hours for the average American to read all the platform agreements to which they are party,[123] how long would it take to monitor every such agreement and analyze the changes thereto when they occur? The task would become Sisyphean.

Modifiable platform terms also foreclose the possibility of a market for terms. Even if any such market existed for terms provided at sign-up, the possibility of competition is obviated as soon as any given platform acquires a meaningful number of users. Once that threshold is crossed, there is little incentive for a platform to refrain from modifying its platform terms to permit every practice on which it originally competed.[124] The most likely outcome is analogous to that predicted by Hotelling's law—instead of a range of competitors offering terms across a

---

121. *See, e.g.*, *Microsoft Services Agreement*, *supra* note 108 ("If you don't agree to the new terms, you must stop using the Services, close your Microsoft account and, if you are a parent or guardian, help your minor child close his or her Microsoft account."); *see also* FACEBOOK, *supra* note 107 ("[I]f you do not agree to our updated Terms and no longer want to be a part of the Facebook community, you can delete your account at any time.").

122. *See, e.g.*, YOUTUBE, *supra* note 109 ("Modifications to this Agreement will only apply going forward. If you do not agree to the modified terms, you should remove any Content you have uploaded and discontinue your use of the Service.").

123. *See* McDonald & Cranor, *supra* note 7, at 565.

124. The flip side of this analysis is set forth by Becher and Benoliel, who point out that firms' ability to unilaterally change the contract disincentivizes consumers from even attempting to find a platform initially offering superior terms. *See* Becher & Benoliel, *supra* note 3, at 692–93 (arguing that unilateral modification "can render the initial contractual promises [firms make] quite meaningless" and noting the possibility that such provisions "can harm competition among firms" because consumers "are unlikely to comparison shop for the best initial contract terms").

continuum of privacy protection, all market participants will eventually converge around a standard set of practices.[125] The privacy practices that have emerged from the market to date leave much to be desired.

And yet the most trenchant critique of the existing privacy paradigm might be that the most problematic uses of data are those that lie in the future. The fundamental disconnect between when consumers provide data and when platforms find novel, useful, and troubling applications for that data renders contractual regulation worthless.[126] Unilateral modification means that platforms can revise platform terms to expressly provide consumer consent to whatever novel collection and use the platform has devised. These provisions allow platforms to sanitize conduct that was not, and could not have been, part of the original expectations of the parties. One might reasonably expect, for instance, that college students happily uploading their photos to Facebook in the early 2000s might have thought twice if they knew that, little more than a decade hence, facial-recognition algorithms trained on such photos would lead to multiple wrongful arrests of Black men based on incorrect detection and matching.[127] Yet the prevailing paradigm allows platforms to manufacture consent to such practices after the fact, even though many, if not most, users would refuse to grant permission for such actions given the opportunity. In the FTC's view, such conduct is forbidden only where platforms "alter their policies and use previously collected data in a manner that materially differs from the terms under which the data was originally collected," and becomes permissible so long as a

---

125. *See, e.g.*, Harold Hotelling, *Stability in Competition*, 39 ECON. J. 41, 52–53 (1929) (demonstrating that if merchant A's location is fixed, merchant B will be incentivized to "set up shop . . . just as close to A as other conditions permit"). It bears emphasis that DuckDuckGo, the one outlier in the top 122 websites that does not subject consumers to unilateral modification of its terms (because it does not have any) is not a significant competitor in its market (search services). At *minimum*, Google handles in approximately twenty-one minutes as many searches as DuckDuckGo handles in a day. *Compare DuckDuckGo Search Traffic*, DUCKDUCKGO, https://duckduckgo.com/traffic [https://perma.cc/7JBH-P4FF] (reporting an average of 99,238,109 searches handled each day by DuckDuckGo in December 2021), *with* Christo Petrov, *The Stupendous World of Google Search Statistics*, TECHJURY, (June 3, 2022), https://techjury.net/blog/google-search-statistics/ [https://perma.cc/LR4Q-VAA8] (reporting that, in 2020, Google processed 6.9 billion searches per day). The presence of a niche player competing on privacy is cold comfort in light of that disparity.

126. *See, e.g.*, Barocas & Nissenbaum, *supra* note 9, at 32 (arguing that "upfront notice is not possible because new classes of goods and services reside in future and unanticipated uses").

127. *See, e.g.*, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/ZWA3-Y3HP] (reporting on the wrongful arrest and imprisonment of Nijeer Parks based on an incorrect facial-recognition match in the third known such case). On November 2, 2021, Meta announced that it was "shutting down the Face Recognition system on Facebook," in part because "[t]here are many concerns about the place of facial recognition technology in society, and regulators are still in the process of providing a clear set of rules governing its use." Jerome Pesenti, *An Update on Our Use of Face Recognition*, META (Nov. 2, 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/ [https://perma.cc/5VP2-9RGF].

platform "first obtain[s] the consumer's consent."[128] Such an approach of course places no limitations on data collected after the platform changes its terms.

The fluidity of terms poses unique problems for privacy protection. Platform terms govern other important consumer issues, with provisions pertaining to warranties, dispute resolution, and so forth. But compared to privacy terms, these provisions are relatively discrete—any change to the terms of a warranty, for instance, would be far easier to notice and understand than would changes to the already vague manner in which firms describe the data they gather and the uses to which they put it.

There is no serious potential for mitigating the complexity of ever-changing platform terms. In theory, for the most popular platforms and services, a relative handful of interested individuals or entities could dedicate the time and resources necessary to keep up with changes to platform terms, summarizing key changes for the rest of the user base.[129] But the modular, fluid nature of devices, platforms, and services governed by those terms represents an unsolvable dilemma for the notice-and-consent regime.

2. Changing Services

What you see is no longer what you buy. Nor can it be. The online services on which countless people daily rely are, of course, dependent on software. Increasingly, so too are the physical devices littering the world's Wi-Fi and cellular networks. From headphones to heaters, coffee machines to cars, it is difficult today to find devices that do not rely on embedded, connected software. That reality further mocks any attempt to rely on contracts for regulation.

Software updates represent a particularly insidious way for platforms to frustrate consumer expectations. The problem stems from two simple truths about software: all software has bugs, and some of those bugs create security risks. Keeping software up to date is a moral imperative in a networked world, the digital equivalent of the need for individuals to keep up to date with vaccinations. Yet the reality of software development means that security updates and "feature" updates cannot feasibly be separated. Thus, changes to software designed to extract more consumer information can be forced on consumers who otherwise would prefer not to give up that information by tying those changes to security fixes. Moreover, the importance of keeping software updated has pushed most software ecosystems toward automatic updating, further limiting the ability of privacy-conscious consumers to control their data. Additional complications arise from the fact that consumers have no way to know what any given software update actually *does*, and software providers tend not to ease that burden by disclosing what they have changed—to say nothing of changes to what those providers are doing on the back end with data gathered from use of the software. And, in any event, providers themselves do not always know what privacy issues their software creates because they rely on third-party components

---

128. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING: BEHAVIORAL ADVERTISING TRACKING, TARGETING, & TECHNOLOGY 9, 19 (2009) (citing *In re* Gateway Learning Corp., FTC Docket No. C-4120, 2004 WL 2618647 (Sept. 10, 2004)).

129. *See, e.g.*, Arbel & Shapira, *supra* note 64.

incorporated into their software that also receive regular, potentially problematic updates. Each of these complications is as implacable as it is incapable of being regulated by contract.

A. Fixing Bugs and Invading Privacy

Software is never perfect and never complete. Efforts to address that reality can be roughly categorized as bug fixing and feature development. The former category tends to benefit both consumers and providers; the latter can be a mixed bag. Unfortunately, as a practical matter the two must be delivered together, opening consumers up to exploitation by software providers.

Software bugs range from mostly harmless[130] to catastrophic.[131] While the typical consumer will likely notice only those bugs that cause software to behave in unexpected or inefficient ways, bugs that create security vulnerabilities are among the most critical. Nevertheless, a consumer might be expected to value fixes to both types of problems. Conversely, software that acquires a reputation for functioning poorly or exposing consumers to security risks is less likely to succeed in the market, giving providers a strong incentive to resolve bugs as they are found.

And the onslaught of software updates suggests they are found frequently. Analysis of the app-update dataset is instructive. On average, the 100 most popular apps on the Google Play Store received updates every 15.5 days.[132] The average time between updates for these popular apps ranged from every 3.7 days to every forty-nine days.[133]

The app-update dataset reveals a blistering pace of updates. Yet regular software updates are not unique to the world of smartphone apps. Even operating-system software for which the update process can be a major disruption, such as Microsoft's Windows, is updated at least once per month.[134]

---

130. For example, some games for the Nintendo Entertainment System contained bugs that allowed the player to enter a "minus world" version of a level that could not be completed. *See, e.g.*, Ethan Gach, *Player Discovers That* The Legend of Zelda *Has a 'Minus World' Too*, KOTAKU (Jan. 3, 2019, 3:00 PM), https://kotaku.com/hacker-unearths-the-legend-of-zeldas-minus-world-1831466758 [https://perma.cc/VQ5W-AJMS].

131. NASA's Mars Climate Orbiter famously burned up in Mars's atmosphere because of a unit mismatch between commands sent to the orbiter and what the orbiter's software expected. *See* NASA, *Mars Climate Orbiter*, NASA SCIENCE, (July 25, 2019), https://solarsystem.nasa.gov/missions/mars-climate-orbiter/in-depth/ [https://perma.cc/28SR-RJB2] (noting that commands were sent to the orbiter in pound-seconds, while the orbiter interpreted the commands in Newton-seconds). The failed project cost $327.6 million. *See* NASA, *Mars Climate Orbiter*, (Apr. 27, 2022), https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1998-073A [https://perma.cc/XM59-JRRP].

132. This figure excludes eighteen apps that had fewer than ten total updates; the average time between updates when including that group was 14.6 days.

133. "Sort Water Puzzle" and "Paramount+," respectively. This range likewise excludes apps with fewer than ten total updates. Taking the crown among that excluded group of eighteen apps, the developers of the app "Monster Box" pushed seven updates at an impressive rate of one every 1.86 days.

134. To minimize disruption and assist IT professionals in managing the update process, Microsoft updates Windows on the second Tuesday of every month, commonly known as

Software updates are not an unalloyed good. Updates have been known to break compatibility for some consumers, or even to cause their devices to cease functioning—a phenomenon known as "bricking" the device.[135] Moreover, reverse engineering of software update code permits bad actors to identify bugs, allowing them to develop exploit code they can use against installations that have not been updated.[136] While the former type of issue can be ameliorated to some extent by better testing, the latter is a necessary tradeoff. Just as with receiving vaccinations, it is thus imperative for consumers to keep software up to date, even at the cost of annoyance and running the risk of causing other problems.

But software providers do not limit themselves to the product they initially release. Indeed, consumers have come to expect that the software they use will receive substantial updates over time.[137] But software providers' self-interest does not always align with consumer interests, leading providers to push updates to products that result in an inferior user experience. Apple provided a classic example when it pushed its own mapping software with the introduction of iOS 6, replacing the popular Google Maps app it had included with previous versions of iOS. While advantageous to Apple from a business perspective, their in-house mapping software failed to stack up to the Google product it replaced in several ways: for example, it dropped public transit directions and was riddled with erroneous locations and names.[138]

Worse still are updates that diminish consumer privacy purely for developers' economic purposes. Grindr furnishes a troubling example. Grindr describes itself as

---

"patch Tuesday." *See* Brian Krebs, *Microsoft Patch Tuesday, December 2021 Edition*, KREBS ON SECURITY (Dec. 14, 2021), https://krebsonsecurity.com/2021/12/microsoft-patch-tuesday-december-2021-edition/ [https://perma.cc/8HQG-PXBB] (describing, inter alia, contents of December 2021 Microsoft Windows updates). Apple's macOS is updated on a more ad-hoc but still regular basis. The current version, Monterey, has received eight updates since its release in October 2021; its predecessor, Big Sur, has received twenty-one updates since its release in November 2020.

135. *See, e.g.*, Jay Peters, *Google Will Replace Home Devices Bricked Due to Latest Firmware Update*, THE VERGE (Oct. 24, 2019, 6:31 PM), https://www.theverge.com/2019/10/24/20931201/google-home-mini-bricking-firmware-update-replace-out-of-warranty [https://perma.cc/LGT6-CBKZ] (noting widespread reports of Google Home and Home Mini devices being rendered inoperable "by an error in an automatic firmware update").

136. *See, e.g.*, Gregg Keizer, *Hackers Now Crave Patches, and Microsoft's Giving Them Just What They Want*, COMPUTERWORLD (May 11, 2014, 9:31 AM), https://www.computerworld.com/article/2489256/hackers-now-crave-patches--and-microsoft-s-giving-them-just-what-they-want.html [https://perma.cc/F6PZ-C8YT] (noting that hackers promptly reverse engineer monthly Windows updates in order to identify security vulnerabilities patched by the updates).

137. *See, e.g.*, Marvin Fleischmann, Miglena Amirpur, Tillmann Grupp, Alexander Benlian, & Thomas Hess, *The Role of Software Updates in Information Systems Continuance—An Experimental Study from a User Perspective*, 83 DECISION SUPPORT SYS. 83 (2016) (finding that consumers prefer feature updates to technical updates and frequent small updates to large, omnibus updates).

138. *See* Charles Arthur, *Apple Maps: Tim Cook Says He is 'Extremely Sorry'*, THE GUARDIAN (Sept. 28, 2012, 10:12), https://www.theguardian.com/technology/2012/sep/28/apple-maps-tim-cook-apology [https://perma.cc/6E8D-YMF6].

"the world's largest social networking app for gay, bi, trans, and queer people."[139] At some point in its more than decade-long existence,[140] Grindr updated its app to transmit certain data to the behavioral advertising platform MoPub.[141] In January 2020, Norway's Consumer Council released a report demonstrating that the Grindr app transmitted sensitive information including the user's age and precise GPS location to MoPub, which then retransmitted that information to third parties bidding to serve an ad to that user.[142] Such practices prove devastating to privacy.[143] After all, a participant in the real-time bidding processes operated by MoPub and other ad platforms need not intend to win the auction in order to receive the private information disclosed by the ad platform to all bidders. Such bidders include, for instance, "Venntel, a government contractor that sells location data to Immigration and Customs Enforcement"—location data it acquires, in part, from bidstream data.[144]

In a startlingly cynical example of consumer exploitation, the computer security firm Avast inserted tracking software into its free, consumer-oriented antivirus products.[145] Avast's advertisements to clients for the tracking data it sold indicated that it could provide: "Every search. Every click. Every buy. On every site."[146] Consumers, of course, install antivirus and antimalware software precisely to defeat this type of tracking, and grant it privileged access to their systems in order to accomplish that task.

The mix of benefit and burden that accompanies software updates creates an implacable problem. A rational consumer might wish to be able to receive security updates for their software while retaining the option to reject feature updates that they do not want, especially features that imperil consumer privacy. In most

---

139. GRINDR, https://www.grindr.com [https://perma.cc/F6RL-PQKF].

140. *See id.* at *About*.

141. *See Out of Control*, FORBRUKERRÅDET, 124–28 (Jan. 14, 2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf [https://perma.cc/S8DY-S8LU].

142. *See id.* (describing behaviors observed during technical testing of the Grindr app).

143. *See, e.g.*, *id.* at 178 ("The collection of data across services and devices allows many of these companies to construct intricate profiles about individual consumers, which can be used to target, discriminate and manipulate people.").

144. Joseph Cox, *Tech Giants Won't Name Foreign Companies They Give US 'Bidstream' Data To*, MOTHERBOARD (Apr. 9, 2021, 9:00 AM), https://www.vice.com/en/article/k78ewv/bidstream-data-google-twitter-att-verizon-foreign [https://perma.cc/7YKH-TJ7A]; *see also* Joseph Cox, *CBP Refuses to Tell Congress How it is Tracking Americans Without a Warrant*, MOTHERBOARD (Oct. 23, 2020, 11:03 AM), https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant [https://perma.cc/5DNH-L439] (reporting that Venntel sold information to the government obtained "from weather, games, e-commerce, and other innocuous apps," along with bidstream data).

145. *See, e.g.*, Joseph Cox, *Leaked Documents Expose the Secretive Market for Your Web Browsing Data*, MOTHERBOARD (Jan. 27, 2020, 9:00 AM), https://www.vice.com/en_us/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation [https://perma.cc/97AW-45CC].

146. *Id.*

circumstances, it is not feasible for developers to fulfill that desire even if they wanted to.

Imagine a developer introduces a new piece of word-processing software called Writr. Version 1.0 is well received and attracts a moderately large userbase. After several months of continued work, Writr's developers prepare an update that fixes several security bugs and also introduces a new cloud-based grammar checking feature that transmits documents to the developer's servers as they are written for automated analysis. Many consumers, concerned about the privacy implications of transmitting all their work to the cloud as they type, agitate for an update that includes only the security fixes. If Writr's developers want to provide that option, they must "fork"[147] the code—creating a version containing only the original code plus security fixes (referred to, perhaps, as version 1.0.1) and a version including both the fixes and the new features (version 1.1). Both the software and userbase are split; the developers must continue working on two different codebases and providing support to each set of customers.

Suppose that, months later, the developers ready another patch full of security fixes as well as a new citation management feature. The previous process repeats, with a new wrinkle: some users of each of the extant versions want just the security patches; some users want the security patches and the new feature; and some users who rejected the grammar-check feature now want both the security patches and the citation management feature. To meet that demand, the developers would have to create versions consisting of (1) the original codebase plus all security patches (1.0.1.1.); (2) the grammar checking update plus the new security patches but without the citation management feature (1.1.1); (3) the full grammar-checking update plus the citation management feature and the new security patches (1.2); and (4) the original codebase plus all security patches and the citation management feature (1.0.2). Both the codebase and userbase have now been split into four groups, each of which presents distinct development and support issues. As development marches on, the situation becomes exponentially more complicated.

Thus, for most software and most developers, catering to demands for separation of security and feature updates is not possible. The choice, then, is between providing nothing but security updates for a given piece of software or bundling security updates and feature updates even when some users might refuse the feature updates if given the opportunity. The socially optimal privacy regime would permit development of new features without giving rise to significant privacy concerns. Notice-and-consent-based regulation cannot provide that regime. Instead, it incentivizes behavior like that discovered in Grindr and other apps.

B. Automatic, Secretive Updates

Consumers are famously recalcitrant about updating software. According to a 2019 study, fifty-five percent of all installed software was out-of-date, with fifteen

147. To "fork" a codebase means to split off a new version of the code from a common development history; it is akin to a single path diverging into two separate paths. The term "fork" has been used this way in software development for decades. *See, e.g.*, Eric Allman, *An Introduction to the Source Code Control System*, SOURCE FORGE (June 1, 2020), http://sccs.sourceforge.net/man/sccs.me.html.

percent of Windows 7 and nine percent of Windows 10 installations also out-of-date.[148] Worse still, millions of people continue to use Windows XP, for which Microsoft officially ended support in April 2014, and Windows 7, for which Microsoft dropped support in January 2020, was still in use on more than *200 million* PCs in January 2021.[149] Companies do not stop updating software because it no longer has bugs; they do so because it is no longer economically viable for them to support the software.

To combat the significant security risk posed by out-of-date software, software providers and app stores increasingly push automatic software updates. At launch, the "Home" edition of Windows 10 had automatic updating automatically and irrevocably enabled.[150] Both Apple's App Store and Google's Play Store automatically update installed apps by default, although both include the option for consumers to turn off automatic updating. Leading web browsers like Chrome and Firefox long ago began automatically updating by default.

Such draconian and prophylactic measures may be warranted by the risks posed by out-of-date software. But, as illustrated above, software developers can and do leverage the imperative of updating to push privacy-threatening changes. When a consumer can wake up to software and devices that suddenly and severely imperil their privacy, it is difficult to contend seriously that they have received what they bargained for.

The update conundrum is further complicated by the impossibility of determining the function of a given update. Particularly where mobile apps are concerned, developers often communicate as little information as possible about the contents of a given update.

When provided, specific information about updates to software is typically communicated in the form of a summary or list of changes; common terms for these documents include "release notes," "patch notes," and "changelogs."[151] But

---

148. *Avast PC Trends Report 2019*, AVAST 7–9, https://cdn2.hubspot.net/hubfs/486579/Avast_PC_Trends_Report_2019.pdf [https://perma.cc/H4K5-888E].

149. Tom Warren, *Windows 7 is still Running on at Least 100 Million PCs*, THE VERGE (Jan. 6, 2021, 11:36 AM), https://www.theverge.com/2021/1/6/22217052/microsoft-windows-7-109-million-pcs-usage-stats-analytics [https://perma.cc/MQQ6-VL5G] (noting analyst findings that Windows 7 remains in use on at least 100 million PCs and "could still be in use by more than 200 million devices worldwide"). Some comfort may be derived from the fact that this comes in well under some analysts' estimates made at the time Microsoft dropped support for Windows 7. *See, e.g.*, Gregg Keizer, *Windows by the Numbers: Windows 10 rolls on past 70%*, COMPUTERWORLD (Nov. 4, 2020, 3:00 AM), https://www.computerworld.com/article/3199373/windows-by-the-numbers-windows-10-resumes-march-towards-endless-dominance.html. [https://perma.cc/4CR3-HJFN] (estimating that Windows 7 would remain in use on 300 million PCs in January 2021).

150. *See* Tom Warren, *Windows 10's Forced Automatic Updates are a Good Idea*, THE VERGE (Jul. 17, 2015, 7:08 AM), https://www.theverge.com/2015/7/17/8987549/microsoft-windows-10-automatic-updates. [https://perma.cc/3CUQ-2Z7P].

151. *See*, *e.g.*, *Release Notes*, GNOME, https://wiki.gnome.org/ReleaseNotes [https://perma.cc/WFL8-SUNG] (Mar. 24, 2021, 11:20 AM) (stating that, for each six-month release, developers of the GNOME user environment will "write release notes describing the major user-visible changes, along with a general description of GNOME"); *Foobar2000 Changelog*, FOOBAR2000, https://www.foobar2000.org/changelog [https://perma.cc/Z8SF-

developers are not generally required to publicly disclose anything about changes to their software, and many do not. While the Google Play Store supports disclosing the changes made with each app update, it does not force developers to do so. Meta, and its subsidiary Instagram, publish no update notes on the Play Store. Apple's App Store does appear to require some information disclosure with updates, but Apple does not appear to police what information developers include. Thus, many developers skirt the requirement. Of the last twenty-five updates to the Snapchat app—the most popular free app on the App Store at the time of analysis—twenty-two feature identical information in the "What's New" field of the app's page in the App Store: "Bug fixes."[152] Similarly, every single one of the most recent twenty-five updates to the Robinhood app, which gives consumers "mobile access to the [securities] markets,"[153] states simply "bug fixes & improvements."

While not every app developer reuses the same language for every update, most provide only some variation on the theme of "bug fixes and performance improvements" and the occasional announcement of a new feature. Of the twenty iOS apps analyzed, only three regularly included even moderately informative descriptions of the changes included in updates, and only in some cases.[154]

Unless an update makes obvious, user-noticeable changes, the typical consumer would be unable to determine *anything* about what the uncommunicative developers of these apps had done. For anything less obvious—such as Grindr's inclusion of code to transmit consumer data to MoPub—it would take a significant degree of effort and technical expertise to figure out what changes the update had wrought. To do so, a consumer would have to isolate, reverse engineer, and analyze the update code—a practice that is probably illegal.[155] And there is no way whatsoever for a consumer to determine what changes are being made on the server side of platforms like Facebook.

Consumers are not the only group who might be surprised by what information their apps are obtaining and disclosing. Many developers rely on third-party tools, delivered via software development kits (SDKs) and application programming

---

4AP4] (providing a detailed list of changes made for each version of Foobar2000 audio player software).

152. Three updates in a row in November 2020 include a different repeated note: "Introducing Sounds! Add music to your Snaps from our curated catalogue or custom record your own Sounds[;] We've made a few updates that make getting around Snapchat easier!"

153. *Our Product*s: *Stocks & Funds*, ROBINHOOD, https://robinhood.com/us/en/about/#our-products [https://perma.cc/NF8T-FS7M].

154. For example, of three updates to the Zoom app in February 2021, two were described only as including "Bug fixes." The third, however, was described as: "Variety of updates: attendee controls for webinars; alternate host feature; zoom room on app; block from specific countries; iOS filters; private chat; SMS for international phone numbers; voicemail notifications; security enhancements and minor bug fixes." The only other apps with a meaningful number of somewhat informative patch notes were Toca Life World and Picsart.

155. *See, e.g.*, *Coders' Rights Project Reverse Engineering FAQ*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/coders/reverse-engineering-faq [https://perma.cc/4F8J-URXL] (discussing potential legal risks of reverse engineering existing under copyright law, trade secret law, the Digital Millennium Copyright Act, and the Electronic Communications Privacy Act).

interfaces (APIs),[156] to perform certain functions in their applications rather than developing such functions from scratch. But these third-party tools can put consumer information at risk.

Both developers and the third-party SDK providers on whom they rely sometimes act out of less-than-pure intent. For example, developers of some period tracking apps included Facebook's advertising SDK in their apps in order to generate revenue. These apps thus communicated information about users' sexual activity, contraceptive use, menstrual cycles, and mood to Facebook via the advertising SDK.[157] A consumer who trusts the app developer to maintain the privacy of their information but does not trust Facebook has their expectations thwarted by such behavior.

In other cases, developers are merely careless, to the detriment of their users. In one typical case, the developers of a popular, free PDF-creation app called CamScanner used a third-party SDK from AdHub to monetize their app. An update to AdHub's SDK introduced a trojan horse virus into the app that could download and install other malicious software without the user's awareness, much less consent.[158] While Google removed the app from the Play Store upon being notified of the issue by security researchers,[159] apps that communicate information to third parties via SDKs continue to thrive.[160]

Software exists in a state of perpetual imperfection. Whether due to security or business demands, developers update software not until they are finished, but until it

---

156. Both SDKs and APIs are ready-made toolsets that provide developers useful functionality, allow them to interface with other services, and the like. The payment-processing service Square provides a helpful illustration to explain the difference between SDKs and APIs: an API is like a recipe for a chocolate cake, while an SDK is like a pre-made cake mix including the recipe in the package. *See What's the Difference Between an SDK and an API?*, SQUARE (Nov. 14, 2018), https://squareup.com/us/en/townsquare/sdk-vs-api [https://perma.cc/96SU-BVN4].

157. *See* Megha Rajagopalan, *Period Tracker Apps Used by Millions of Women Are Sharing Incredibly Sensitive Data With Facebook*, BUZZFEED NEWS (Sept. 9, 2019, 12:03 PM), https://www.buzzfeednews.com/article/meghara/period-tracker-apps-facebook-maya-mia-fem. [https://perma.cc/5552-DLPT].

158. *See* Sergiu Gatlan, *Trojan Dropper Malware Found in Android App with 100M Downloads*, BLEEPING COMPUT. (Aug. 27, 2019, 11:00 AM), https://www.bleepingcomputer.com/news/security/trojan-dropper-malware-found-in-android-app-with-100m-downloads/. [https://perma.cc/D3FX-5D6N].

159. *Id.*

160. Grindr, for example, continues to note in its privacy policy that "[t]o maintain and improve the Services, we collect Personal Information such as user activity, hardware and software information, cookies, and leverage other technologies such as web beacons, software development kits (SDKs), local storage, and log files." *Grindr Privacy and Cookie Policy*, GRINDR, https://www.grindr.com/privacy-policy/?lang=en-US [https://perma.cc/N9R2-AKXF]. Similarly, the privacy policy for HBO Max—a service with an associated app that received updates approximately monthly in the period analyzed—provides that WarnerMedia may use "cookies, web beacons, pixels, SDKs, or similar technologies to collect data and show advertisements on our Digital Services and on third party websites and applications over time." *HBO Max Privacy Policy*, HBO MAX, https://www.hbomax.com/privacy/en-us [https://perma.cc/V7L7-SWBL].

is no longer economically feasible to continue. As a result, a given piece of software—or a device dependent on embedded software—may cease to resemble the version originally obtained by a consumer. Existing critiques of platform terms do not speak to this reality because of their focus on the initial platform terms. It is difficult to conceive of an *ex ante* contract solution to the problem of developers—sometimes inadvertently—slipping privacy-destroying code into updates to their software, or of enabling consumers even to begin to understand how updates may affect their privacy.

3. Changing Ownership

Even if code could be made perfect, secure, and immutable, there would remain the problem of data control. A consumer might feel comfortable entrusting their data to a particular platform, perhaps one that has made extensive reassurances about its privacy practices. But the consumer is powerless to stop that platform from being acquired by another, less savory, entity.

That scenario is distressingly likely. According to a 2019 survey by Silicon Valley Bank, approximately fifty percent of executives at Silicon Valley startups expect their companies to be acquired.[161] While those executives might view such an acquisition as a rosy outcome, it can be deeply troubling to consumers of their products and services, who might find themselves indirectly having given their private information to companies that do not respect their privacy.

Google's acquisition of Fitbit led to such concerns. Fitbit for years sold a line of smartwatches and fitness trackers that, in conjunction with Fitbit's apps, measure and record various types of information about their users, including: "stress management score," electrocardiograms, "Oxygen Saturation (SpO2 Monitoring)," "On-Wrist Skin Temperature Sensor," "24/7 Heart Rate Tracking," "Breathing Rate," "Menstrual Health Tracking," and "Sleep Stages & Sleep Score," among a host of other deeply personal information.[162] Informed Fitbit purchasers presumably trusted the company enough to track and store that kind of information, and perhaps with good reason: at least one analysis of Fitbit's pre-acquisition privacy policy and practices rated Fitbit in a tie for first in terms of privacy protection among wearable-technology providers.[163] Unsurprisingly, Google's acquisition of the company led many consumers to fear for their privacy.[164]

---

161. *See* Peterson, *supra* note 14. Indeed, the pace of acquisitions-as-exit for startup companies has dramatically increased over the last three decades. *See* Mark A. Lemley & Andrew McCreary, *Exit Strategy*, 101 B.U. L. REV. 1, 18 (2021).

162. These features are advertised on the product page for Fitbit's Sense smartwatch. *See Features*, FITBIT, https://www.fitbit.com/global/us/products/smartwatches/sense?sku=512BKBK [https://perma.cc/7CHG-Q88K].

163. *See* Sophie Charara & Husain Sumra, *We Read Your Wearable Tech's Privacy Policy so You Don't Have To*, WAREABLE (May 25, 2018), https://www.wareable.com/wearable-tech/terms-and-conditions-privacy-policy-765 [https://perma.cc/NM3P-KWC8] (rating Fitbit and Apple privacy policies as the strongest, ahead of Samsung, Garmin, Under Armour, Google, and Xiaomi).

164. *See, e.g.*, Kari Paul, *'Tossed My Fitbit in the Trash': Users Fear for Privacy After*

While Fitbit and Google attempted to assuage consumers' fears by announcing they would continue to respect consumer privacy,[165] they are not bound to do anything of the sort. Rather, Fitbit's privacy policy at the time of the Google acquisition announcement expressly provided for an acquisition in terms that obligated it to do very little, if anything, to protect consumer information.[166] The only firm commitment in the policy is to provide notice to consumers "before transferring any personal information to a new entity."[167] A spokesperson's puffery is neither enforceable nor comforting to consumers whose health information is about to be sold to Google. The same situation will play out in the pending Amazon acquisition of One Medical: its privacy policy likewise provides for the transfer of personal data, including health data, in the event of an acquisition.[168]

Such terms are commonplace. Analysis of the same set of platform terms discussed above[169] reveals that nearly half expressly provide that consumer information may be transferred in the event of a sale of the business, with no requirement that consumers even be notified of the sale.[170] Meta's data policy, for example, states that "[i]f the ownership or control of all or part of our Products or their assets changes, we may transfer your information to the new owner."[171]Netflix's privacy policy gestures toward consumer protection, but in terms

---

Google Buys Company, THE GUARDIAN (Nov. 6, 2019, 3:07 PM), https://www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data [https://perma.cc/J326-TL4J].

165. *See, e.g.*, *id.* (noting Fitbit's statement that "[s]trong privacy and security guidelines have been part of Fitbit's DNA since day one, and this will not change").

166. *See Previous Privacy Policies*, FITBIT, https://www.fitbit.com/us/legal/previous-terms/09182018 [https://perma.cc/524U-A3E4] ("If we are involved in a merger, acquisition, or sale of assets, we will continue to take measures to protect the confidentiality of personal information and give affected users notice before transferring any personal information to a new entity.").

167. *Id.* Its most recent privacy policy, effective August 16, 2021, does not alter this provision. *See Fitbit Privacy Policy*, FITBIT, https://www.fitbit.com/global/us/legal/privacy-policy [https://perma.cc/3FK5-FU5J].

168. *See 1Life Healthcare, Inc. Privacy Policy*, ONE MED., https://www.onemedical.com/privacy/ [https://perma.cc/SDZ7-LGMV] ("If we are acquired by a third party as a result of a transaction such as a merger, acquisition or asset sale . . . some or all of our assets, including your Personal Information, may be disclosed or transferred to a third-party acquirer in connection with the transaction."). While the privacy policy states that it does not apply to "Protected Health Information," as that term is used in the Health Insurance Portability and Accountability Act, HIPAA permits transfers of such information to a "business associate" pursuant to a "business associate contract or other arrangement." *See* 45 C.F.R. § 164.502(a)(3) (2020).

169. *See supra* Section II.A.

170. Of the 122 unique sets of platform terms analyzed, fifty-nine expressly provide for transfer of consumer information in the event of a merger or similar business transaction; such a right is implicit in many others. Microsoft and Yahoo, whose platform terms account for several of the top 150 websites, respectively, include such terms. Among the remainder, forty-three are silent on the issue.

171. *Meta Data Policy*, FACEBOOK, https://m.facebook.com/privacy/policy/version/20220104/ [https://perma.cc/YN3R-PCK5] (Jan. 4, 2022).

that are so vague as to be meaningless: "In connection with any reorganization, restructuring, merger or sale, or other transfer of assets, we will transfer information, including personal information, provided that the receiving party agrees to respect your personal information in a manner that is consistent with our Privacy Statement."[172] A consumer who objects to the practices of the new owner has no recourse except, possibly, to request deletion of all the data held by an entity before it is transferred to an acquirer—a right that often does not exist[173] and may be found unenforceable even if granted by law.[174] Indeed, some law moves in the other direction. Virginia's recently enacted Consumer Data Protection Act specifically exempts data transfers in mergers and acquisitions, among other transactions, from its definition of "[s]ale of personal data."[175]

At the beginning of the relationship between a consumer and a platform, piece of software, or device, the consumer is presented with a set of platform terms and an idea of what the platform, software, or device will do. After those terms are "accepted," all bets are off. The terms themselves may be changed without any notice to the consumer. Platforms and developers may add or remove features, possibly compromising consumer privacy, removing valuable functionality, or both. Under-the-hood or back-end changes take place constantly, generally with no meaningful notice to consumers about what has changed and no opportunity for consumers to figure it out for themselves. Those hidden changes might also include the addition of prefab code from another entity—one with which the consumer has no relationship—that allows third parties to access consumer information or compromise the security of consumer devices. And whichever entity ends up in possession of consumer information might end up being sold, data and all, to an entity offering inferior privacy protection.

Under existing U.S. privacy regulations, absent extraordinary circumstances, all this conduct is perfectly legal because of the consumer's initial "consent" to the terms.[176] But it goes well beyond credulity to suggest that this relationship can be reduced, ex ante, to a writing. Only a clairvoyant consumer would even have a chance.

---

172. *Netflix Privacy Statement*, NETFLIX, https://help.netflix.com/legal/privacy [https://perma.cc/PP47-FUBU] (Nov. 2, 2021).

173. For example, Netflix allows consumers to request deletion of their data but notes that it "may reject requests that are unreasonable or not required by law, including those that would be extremely impractical, could require disproportionate technical effort, or could expose us to operational risks such as free trial fraud." *Id.*

174. *See, e.g.*, Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017) (holding that consumer lacked standing to challenge cable company's failure to delete consumer's personal information as required by the Cable Communications Policy Act); *see also* Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925 (8th Cir. 2016) (same).

175. *See* 2021 Va. Acts 2 (providing that "[t]he disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or transaction in which the third party assumes control of all or part of the controller's assets" does not constitute the "[s]ale of personal data").

176. With the possible exception of knowing inclusion of malicious software, which would seem to violate the Computer Fraud and Abuse Act. *See, e.g.*, 18 U.S.C. § 1030(a)(5)(A) (criminalizing "the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization").

III. PATHS TO PRIVACY PROTECTION

The dynamic nature of modern software, services, and devices renders the equally malleable terms that govern their use strange creatures. Courts typically treat platform terms as enforceable contracts, and arguments about enforceability most frequently invoke the contractual doctrine of unconscionability.[177] Regulators, meanwhile, are empowered to punish substantial deviations from contractual authorization. Yet for all the bluster that might accompany a successful lawsuit or major FTC enforcement action, platforms' threats to privacy grow only more dire.

Evaluating platform terms, and the subjects thereof, in the full context of their unilateral fluidity requires abandoning the notice-and-consent paradigm. This Part shows first that, contrary to their treatment in the case law, platform terms are best understood not as contracts but as symbols demanded via a de facto licensing regime overseen by both regulators and courts. While neither courts nor regulators would describe it as such, this understanding better reflects the reality of how firms draft platform terms and helps to explain the content of these documents. The result of this system is an almost unfettered right of platforms to appropriate consumer information, subject only to recitation of certain magic words in the platform terms and, if challenged, a court's certification that a given set of terms is not unconscionable—and that only if the platform behaves so egregiously as to draw the attention of a regulator or a suitably large potential class.

Consent is both the linchpin of the existing contractual regime and an impossibility in the circumstances. An individual cannot meaningfully consent to conduct regulated by platform terms wherein both the terms and the subject matter can be changed by the counterparty in its sole discretion, at any time, without any notice to the individual. But reliance on the illusion of consent—driven by adherence to the contractual model of the consumer-platform relationship—helps explain the total failure of existing privacy regulation to mitigate the rise of ever more intrusive software, services, devices, and platforms. Effective privacy regulation must rely on a different approach; contract cannot bend far enough to encompass the reality of the consumer-platform relationship.

The previous Part demonstrated the practical challenges to the notice-and-consent approach to privacy regulation. This Part builds on that analysis to demonstrate the theoretical irrelevance of any regulatory scheme grounded in that paradigm. Part III.A draws on contract theory to show that consumers are not, in any real sense, the counterparties to platform terms, although they are nominally so deemed. Rather, platform terms are drafted with regulators and courts as the true counterparties. Part III.B extends that analysis to consider whether it is ever possible to consent to the practices governed by platform terms. Finally, Part III.C explores the futility of existing approaches, and private ordering more generally, as a means of providing privacy protection.

---

177. *See, e.g.*, Becher & Benoliel, *supra* note 3, at 688 (noting that "courts often enforce contracts that allow firms to unilaterally amend their agreements"); *see also* Song Fi, Inc. v. Google Inc., 72 F. Supp. 3d 53, 63 (D.D.C. 2014) (finding YouTube's terms of service, which included unilateral modification provision, to be enforceable and rejecting argument that terms were unconscionable because they were not "so outrageously unfair as to shock the judicial conscience") (quotations omitted).

A. Consumers as Absentee Counterparties

One clear implication of this Article is that even though existing regulation treats consumers and platforms as having entered into contracts, one party—the consumer—is virtually absent.

Contract theorists have long explored the ways in which the law shapes contract terms.[178] In many cases, contract law encourages private ordering, but sets some limits on its use. For example, contract law expressly prohibits parties from contracting over certain subjects[179] and uses doctrines such as unconscionability and the implied covenant of good faith and fair dealing to further limit allowable contracting.[180] In the context of privacy, law's influence on contract drafting was evident leading up to the effective dates of recent European and California privacy laws: platforms far and wide revised their privacy policies en masse to address new regulations.[181]

Individual consumers on the other end of those policies, of course, had nothing to do with those revisions. As discussed in Part I, they lack the time, training, and capacity to engage with platform terms in any meaningful way. And in reality, nobody *wants* consumers to do so. If people across the world suddenly took it upon themselves to read all the platform terms to which they are nominally a party, and started keeping tabs on any updates thereto, all other human activity would grind to a halt. Quite literally, nobody has the time to do it.

Who then do platforms believe will read, negotiate, and agree to their platform terms? Cathy Hwang and Matthew Jennejohn have shown that firms consider regulators the primary audience for platform terms and attempt to draft terms that maximally favor themselves without crossing whatever lines they perceive regulators to have drawn.[182] In-house counsel know that the only real audiences for the platform terms are the FTC, judges, and plaintiff's counsel, and they draft accordingly.[183]

---

178. *See, e.g.*, Robert H. Mnookin & Lewis Kornhauser, *Bargaining in the Shadow of the Law: The Case of Divorce*, 88 YALE L.J. 950 (1979) (exploring the impact of legal rules and procedures shape the contract-bargaining process).

179. *See, e.g.*, Cathy Hwang, *Faux Contracts*, 105 VA. L. REV. 1025 (2019) (describing some types of contracts that are legally non-enforceable, with parties therefore entering into "faux contracts"—documents that have the appearance of binding, legally enforceable contracts but that are not so).

180. *See, e.g.*, Alan Schwartz & Robert E. Scott, *Precontractual Liability and Preliminary Agreements*, 120 HARV. L. REV. 661, 664 (2007) (describing the role of the implied covenant of good faith and fair dealing in preliminary agreements entered into between sophisticated business parties).

181. For example, Jens Frankenreiter has shown empirically that many websites changed their policies in the months around the effective date of the GDPR, albeit not necessarily to the extent of adherence to the GDPR outside of Europe. *See* Jens Frankenreiter, *The Missing "California Effect" in Data Privacy Law*, 39 YALE J. REGUL. (forthcoming 2022) (manuscript at 39–42) (reporting the results of text analysis of privacy policies from April–July 2018).

182. *See* Cathy Hwang & Matthew Jennejohn, *Contractual Depth*, 106 MINN. L. REV. 1267, 1291–92 (2022) (discussing interviews with in-house counsel responsible for creating terms of service and privacy policies for internet companies).

183. One in-house lawyer interviewed by Hwang and Jennejohn deemed regulators "the

With those audiences in mind, firms are incentivized to draft terms in very particular ways that contribute to the readability crisis. In practice, regulators tend to demand inclusion of specific language in platform terms, regardless of potentially increasing length and complexity.[184] Including such specific terms does not, of course, have any actual effect. Rather, the purpose and effect are merely "placating the attorney general."[185]

Elsewhere, platforms insert particular terms to achieve particular goals that have nothing to do with consumer interests. In one cynical example, Craigslist briefly introduced a new provision in its platform terms that granted it an exclusive license to the copyright in user-created classified ads posted to the platform. It did so for one specific purpose, completely unrelated to its relationship with the nominal counterparty to the terms: to obtain statutory standing to sue a competitor that scraped Craigslist's classified ads for copyright infringement.[186] The judges of the Northern District of California and the Ninth Circuit constituted the entire audience for that term.

Viewed in this light, platform terms exemplify "legal endogeneity"—a process in which private, regulated entities replace the substantive goals of regulation with mere symbols of compliance.[187] Long, complex, unreadable, unilaterally modifiable platform terms reciting the magic words dictated by regulators and precedent are nothing if not symbolic: they do not protect the consumer, although the preambles usually recite that as their purpose,[188] but instead allow the platform to check a box and avoid liability.

It would be one thing if regulation of these documents were merely one aspect of a multifaceted regulatory approach. But under the notice-and-consent regime, regulation appears to stop at the "I agree" checkbox. The FTC, which has authority to regulate these issues, pursues only a handful of privacy-related cases every year,[189]

---

only audience that mattered," while viewing "plaintiff's lawyers and judges [that will decide those cases]" as of secondary importance. Accordingly, when drafting an automatic subscription-renewal term, they "did exactly what the FTC wanted." Another in-house lawyer stated that their "outside counsel says that you draft these not for the consumer but for the FTC and class action plaintiffs." *See id.*

184. *See, e.g.*, *id.* at 1300 (quoting an in-house attorney at an internet company regarding the design of terms of service and privacy policies who noted that "if a regulator doesn't see the exact words they're looking for, they'll ask for it to be inserted").

185. *Id.* at 1301.

186. *See* Craigslist, Inc. v. 3Taps, Inc., 942 F. Supp. 2d 962, 973–74 (N.D. Cal. 2013) (holding that Craigslist could sue for copyright infringement only for user posts made "from July 16, 2012 through August 8, 2012," the period during which Craigslist included the exclusive-license provision in its terms of service).

187. Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 776 (2020).

188. *See, e.g.*, *Google Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en-US [https://perma.cc/R9JP-J55C] ("When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.").

189. *See* Waldman, *supra* note 187, at 797 (noting that "by the FTC's own count, the agency averages only ten privacy-related cases per year, limiting the sources lawyers have from which to glean lessons and find clarity").

and courts are notably hostile to privacy litigation.[190] Indeed, the dominant mode of federal regulation is in fact self-regulation, with the FTC doing little to constrain the means by which firms implement privacy protection.[191]

At most, then, platform terms function as lightly regulated licenses to engage in wholesale appropriation of consumer information. They implement what Danielle Citron calls the "collection imperative"—the drive by firms and governments to collect as much information about as many people as they possibly can.[192] Courts and regulators appear happy to bless any platform terms that arguably provide notice of a firm's practices and include whatever particular language the regulators currently prescribe. Nobody else—including consumers, the nominal counterparties to these contracts—has a seat at the table. In the resulting paradigm for data collection and dissemination, anything goes.

B. The Impossibility of Consent

Even in light of the intractable problems with notice, the temptation remains to make consent the linchpin of privacy regulation. Platforms provide consumers with products and services that those consumers want, and most seem content to pay with access to their data. The baseline position of American jurisprudence is that they are free to do so.[193] But that position is only tenable if consent is meaningful. In the context of platform terms, it is not, and it cannot be.

Kim distills three common conditions underlying legal determinations of consent across numerous areas in the course of developing a "consentability" framework: "an intentional manifestation of consent, knowledge, and volition/voluntariness."[194] The consumer-platform relationship fails the test. True, as discussed in Part I, the legal question of manifestation of intent has been settled in favor of the notice-and-consent paradigm. But it is not necessary to fight that conclusion because platform terms fall forever short on knowledge and voluntariness.

It is commonplace among scholars, and even some courts,[195] that it is not feasible for individuals to understand the initial set of platform terms. In Kim's framework,

---

190. *See* Haley, *supra* note 46 (finding that courts routinely dismiss privacy litigation for lack of standing); *see also* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018) (discussing judicial reticence to recognize privacy harms as real harms).

191. *See, e.g.*, Waldman, *supra* note 187, at 816 (noting that "[t]he FTC . . . defers to industry practices in the area of data security").

192. Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1140–41 (2018) (identifying features of the "collection imperative" including collection of "information about consumers' likes and dislikes, strengths and weaknesses"; "individuals' searches, purchases, musings, and wish lists"; "video streams from public and private security cameras, images from license-plate readers, and data from government and private databases").

193. *See, e.g.*, KIM, *supra* note 51, at 7 (noting that "[i]n societies which value individual freedom, consent plays a singular role . . . . There is consensus that consent is legally and ethically transformative.").

194. *Id.* at 9.

195. *See In re* Facebook, Inc. Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 791 (N.D. Cal. 2019) ("[T]he parties agree that California law requires the Court to pretend that

satisfaction of the knowledge condition requires both that "[t]he consenting party must have access to the information in a form and at a time which helps that party *understand* material and relevant information and the consequences of consent," and "[t]he presentation of the information must take into account the realities of how humans make decisions in given contexts."[196] Even assuming that humans are rational actors and that some regulatory intervention, such as the "nutrition label" approach currently in vogue, could satisfy these conditions at the time of initial consent, neither condition can *ever* be satisfied in light of the fluidity of terms, subject, and parties inherent in the consumer-platform relationship.[197] The volume of terms and the pace of change is such that their meaning is ascertained for the first time, if ever, by a court construing whatever set of terms applied at the time of a certain challenged activity. The prevalence of provisions placing the burden on consumers to monitor platform terms for changes makes a mockery of the inquiry. And decades of social science demonstrate that humans are not rational actors, a fact well known to platforms using dark patterns to sway individual behavior.[198]

That type of exploitation frustrates the voluntariness condition as well. An individual who has been induced by misleading design to click a button purporting to manifest their assent cannot be said to have voluntarily consented. But even the clearest, least misleading "I agree" button often fails to clear the bar because individuals have no real choice.[199] With each passing day, daily life grows more tightly intertwined with a number of platforms—a number that shrinks as industry consolidation continues unchecked. As the Supreme Court noted in *Riley v. California*, "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[200] Following T-Mobile's acquisition of Sprint, three companies (AT&T, Verizon, and T-Mobile) controlled eighty-seven percent of the market for cell phone service in the United States.[201] Microsoft

---

users actually read Facebook's contractual language before clicking their acceptance, even though we all know virtually none of them did. Constrained by this fiction, the Court must analyze the relevant contractual language to assess whether the users 'agreed' to allow Facebook to disseminate their sensitive information in the ways described in the lawsuit.").

196. KIM, *supra* note 51, at 124.

197. *Cf.* Fowler et al., *supra* note 82, at 41 ("Even if consumers recognized the risk of changes to the contract in the abstract, assessing how likely an adverse change sometime in the future might be would be extremely difficult.").

198. KIM, *supra* note 51, at 125 (noting the obstacles posed by "the limits of human cognition and human susceptibility to manipulation and distraction"); *see also supra* Section I.C.

199. KIM, *supra* note 51, at 129 (arguing that "[i]f there are no available alternatives, the condition of voluntariness is deficient . . . . While the consent-seeker may not be physically forcing the individual to *take it*, the option of *leave it* may not be a realistic one.").

200. 573 U.S. 373, 385 (2014); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (noting that "[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales").

201. *See* Ernesto Falcon, *The T-Mobile and Sprint Merger is Blatantly Anticompetitive*, ELEC. FRONTIER FOUND., https://www.eff.org/deeplinks/2019/07/t-mobile-and-sprint-merger-blatantly-anticompetitive [https://perma.cc/8W5L-A8SF] (discussing market share of major

Windows runs 87.56% of desktop computers,[202] and one would be hard-pressed to purchase a new desktop or laptop running something other than Windows or MacOS. Some estimate Facebook's share of the social media market at sixty-four percent—rising to seventy-three percent if one also includes the Meta-owned Instagram.[203] Just two companies (Comcast and Charter) account for more than eighty percent of U.S. cable broadband subscribers, and three (AT&T, Verizon, and CenturyLink) likewise account for more than eighty percent of wireline broadband subscribers.[204] Those figures come as little surprise in light of the fact that "at least 83.3 million Americans can only access broadband through a single provider."[205] For most people, these are not choices.

The changes that would be necessary to enable meaningful consent to platform terms is unimaginable. Simply to solve the knowledge issues would essentially require eradicating platform terms entirely, and further require platforms to disclose in painstaking detail every aspect of their code every time they make a change.[206] To resolve the problem of voluntariness would require not only unwinding decades of mergers and acquisitions but also breaking up market-dominating firms like Microsoft and Comcast.

None of that will happen. The hurdles to meaningful consent to platform terms cannot be cleared. "Notice and consent" is, and always has been, an illusion. In Kim's framework, it is necessary to consider the significance of the "autonomy interest" threatened by an act of consent to determine if the act is consentable.[207] Others have argued convincingly that privacy interests are paramount to protecting the public good.[208] But the obstacles to both notice-and-consent identified in this

---

cell phone service providers).

202. Ali Arslan, *7 Reasons Why Linux Isn't Dominating the Desktop OS Market*, MAKEUSEOF (Apr. 26, 2022), https://www.makeuseof.com/reasons-linux-isnt-dominating-desktop-market/ [https://perma.cc/LGV4-8QTF] (discussing market share of various desktop operating systems).

203. *See Leading Social Media Websites in the United States as of September 2022, Based on Share of Visits*, STATISTA, https://www.statista.com/statistics/265773/market-share-of-the-most-popular-social-media-websites-in-the-us/ [https://perma.cc/U7EU-X7FY].

204. *See About 2,950,000 Added Broadband from Top Providers in 2021*, LEICHTMAN RSCH. GRP. (Mar. 7, 2022), https://www.leichtmanresearch.com/about-2950000-added-broadband-from-top-providers-in-2021/ [https://perma.cc/GL26-MGYS].

205. Christopher Mitchell & Katie Kienbaum, *Report: Most Americans Have No Real Choice in Internet Providers*, INST. FOR LOC. SELF-RELIANCE (Aug. 12, 2020), https://ilsr.org/report-most-americans-have-no-real-choice-in-internet-providers/ [https://perma.cc/2W7N-ZZ5P] (summarizing key findings of report on broadband access in the United States).

206. Individuals would, of course, also somehow need to have the time and knowledge to parse all that code.

207. *See* KIM, *supra* note 51.

208. Julie Cohen, for example, has argued that "the capacity for critical subjectivity shrinks in conditions of diminished privacy," and so too does "the capacity for democratic self-government." *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013) (arguing that privacy intrusions including widespread surveillance curtail the ability of citizens "to form and pursue meaningful agendas for human flourishing"). That the most significant public outcry over privacy intrusion—reaction to the Cambridge Analytica scandal—relates

Article render unnecessary any such weighing of interests. If the goal of any legislative or regulatory reform is to protect privacy, notice-and-consent can have no role.

C. Private Ordering's Futility

If not notice-and-consent, then what? Deep exploration of an alternative regulatory scheme is beyond the scope of this Article. But a few words on the broad contours of a successful privacy-protection paradigm—on whether there is room for private ordering—are in order.

Private ordering cannot avoid the obstacles to consentability posed by fluid terms, services, and parties. The market has not provided competition on the basis of either practices or terms, and, as discussed in Part I, there is every reason to think that it never will. Successful platforms possess a monstrous power advantage not only over their users but over any potential competitors, and that advantage grows the less the platform respects consumer privacy. No Meta competitor will—or *can*—rise to Meta's level without leveraging every shred of data it can collect as Meta does.

Nor would assigning individuals a property right in their data lead to meaningful protection. Whether to treat data as property has animated debate for decades.[209] In light of the fluidity of the consumer-platform relationship, such a regime would amount to notice-and-consent by a different name. Platforms would revise their terms to require assignment of rights to an individual's data as the price of entry; individuals, if they even knew they had been granted such a right, would neither notice the change in terms nor have any real option but to accept.

To protect individual privacy, the only workable approach is direct regulation of data collection, use, and transfer. There is no one-size-fits-all rule to be deployed—for instance, how to regulate access to genetic information and home addresses poses different problems requiring different solutions. Further research is needed to explore the contours of such an approach.

CONCLUSION

Existing critiques of the platform-terms paradigm identify numerous issues with that regime, boiling down to the difficulty an individual would encounter in trying to read and understand to what they were consenting in a set of platform terms. These text-focused critiques are too narrow. By focusing on the fluidity of terms, services, and ownership post-"contracting," this Article exposes the futility of trying to correct the failings of platform terms in service of prolonging the notice-and-consent paradigm of privacy protection. Effective privacy regulation cannot emerge from a

---

to election interference confirms Cohen's thesis. Others have likewise recognized the value of privacy in enabling individual independence. *See, e.g.*, Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 38 (2021) (arguing that "[p]ersonal data can readily be used to affect reputations, shape decision-making, and influence behavior. In the wrong hands, personal data can be used to cause great harm to people.").

209. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2057 (2004) (noting disagreement over whether to treat data as property and collecting citations).

regime seeking to solve complex, dynamic problems with an ex ante writing that is immediately out of date, and the stakes are too high to continue tinkering with privacy regulation that relies on private ordering. Meaningful privacy protection requires, and demands, direct regulation of data collection and use.