Harvard Journal of Law & Technology
Volume 37, Number 3 Symposium 2023

DOES PRIVACY WANT TO UNRAVEL?

*James C. Cooper**

ABSTRACT

Firms are not shy about disclosing their low prices to attract consumers, but they seem to hesitate when it comes to their data practices. If data is increasingly the price we pay, this is surprising. Before we pronounce the meager evidence of unraveling as a symptom of a market failure, however, we need further investigation. We need to know which equilibrium we are in — one in which disclosure is consistent with consumer preferences; a lemons market, in which asymmetric information plagues consumers and firms and keeps them from the privacy they want; or something in between. That is, we need to know if privacy even wants to unravel. Regulation might be appropriate when (1) there is broad agreement that the conduct at issue is harmful, and (2) the government has sufficient information to craft a correct standard. For all other cases, it is preferable to at least attempt a market allocation of data practices. This could be accomplished by providing the FTC with tools to transform what consumers perceive as cheap talk into credible commitments. Chief among them would be the ability to levy penalties sufficient to deter deception over privacy, while also signaling a reluctance to seek monetary remedies for good faith attempts to make privacy claims more understandable to consumers.

* Professor of Law and Director, Program on Economics & Privacy, George Mason University, Antonin Scalia Law School. I thank participants at the *Harvard JOLT*-UIowa IBL Symposium: Beyond the FTC for comments and Sam Bellet for excellent research assistance.

TABLE OF CONTENTS

I. INTRODUCTION

If privacy is the price we pay to access so many things, why are firms so hesitant to talk about it? While consumers can easily compare the prices of IKEA and Pottery Barn bookcases, they are unlikely to be able to assess how these stores handle consumer data because this information resides in incomprehensible privacy policies. This is puzzling because the well-known "unraveling result" suggests that firms have strong incentives to make consumers understand elements of their data handling that are likely to attract new customers. Economic theory generally predicts that as long as firms can credibly (and at a sufficiently low cost) convey information about their product that makes it appear more attractive vis-à-vis at least one competitor, they will.[1] Yet, although there is no a priori reason why IKEA cannot tout both the affordability of its Billy Bookcase *and* what happens to the information it collects when you purchase one, we see only the former.[2]

Despite strong incentives to report privacy practices as long as they are not the "worst," efforts at informing consumers are worthless if consumers do not believe what they hear. Privacy is probably best

1. The seminal work in developing the unraveling result can be traced to W. Kip Viscusi, *A Note on 'Lemons' Markets with Quality Certification*, 9 BELL J. ECON. 277 (1978); *see generally* Sanford J. Grossman & Oliver D. Hart, *Disclosure Laws and Takeover Bids*, 35 J. FIN. 323 (1980) (describing how when transaction costs are zero, it is optimal for the seller to disclose the product's quality); Sanford J. Grossman, *The Informational Role of Warranties and Private Disclosure about Product Quality*, 24 J.L. & ECON. 461 (1981) (describing situations where sellers have an incentive to share information about their products' quality); Paul R. Milgrom, *Good News and Bad News: Representation Theorems and Applications*, 12 BELL J. ECON. 380 (1981) (describing models for how markets respond to "favorableness" news).

2. *IKEA TV Spot, 'Why We Make: $49,'* ISPOT.TV (Aug. 4, 2020), https://www.ispot.tv/ad/n_m2/ikea-why-we-make [https://perma.cc/U2BZ-Y6SK].

described as a credence attribute: although consumers *sometimes* find out when firms do not live up to their privacy promises, the absence of bad news does not necessarily mean that firms are keeping their word.[3] What is more, unraveling rests on firms knowing more about the relative quality of their product than consumers do — an assumption that may work for furniture but may not for data practices. Finally, consumers need to respond favorably to good news about the attribute in question. To the extent that privacy and quality in other dimensions are negatively correlated, the demand response from favorable privacy reports may be insufficiently large to make costly disclosure worthwhile.[4]

The Federal Trade Commission ("FTC") has spent the past quarter century trying to facilitate privacy unraveling under a so-called "notice-and-choice" approach.[5] This type of light-touch regulation is designed to preserve consumer choice, not substitute for it, by correcting faulty information flows. Credible disclosure about privacy can lead to both static and dynamic efficiency gains. First, in a static sense, if consumers can distinguish low-privacy firms from high-privacy firms, they can better sort according to their preferences. Second, in a dynamic sense, the ability to provide credible information about privacy practices can also promote competition over this dimension.

The problems with the FTC's approach have been recognized for some time. Most serious is the lack of an effective remedy to adequately deter deception, which is key to promoting unraveling.[6] Further, privacy law scholars have long viewed the notion of consent in the notice-and-choice model as fiction given the complexity and uncertainty surrounding the use of consumer information.[7] There seems to be a view in ascendency that the notice-and-choice framework is dead. Indeed, the FTC Chair recently pronounced as much with the release of the

---

3. *See* Michael R. Darby & Edi Karni, *Free Competition and the Optimal Amount of Fraud*, 16 J.L. & ECON. 67, 68–69 (1973) (defining credence qualities as those that "cannot be evaluated in normal use" because the consumer may not be able to evaluate the causal link between the promised product and the promised outcome).

4. For a discussion of the relationship between privacy and quality, see James C. Cooper & John M. Yun, *Antitrust and Privacy: It's Complicated*, 2022 U. ILL. J.L. TECH. & POL'Y 343 (finding a negative relationship between privacy grades and user ratings).

5. *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS at 60–64 (Mar. 2012), at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [perma.cc/5EWP-67KF]; *see also* Section II.A., *infra* (describing the FTC's privacy enforcement).

6. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022); James C. Cooper & Bruce H. Kobayashi, *Equitable Monetary Relief Under the FTC Act: An Opportunity for a Marginal Improvement*, 83 ANTITRUST L.J. 645, 668–69 (2021).

7. Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1885 (2013).

FTC's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.[8]

If we are to move beyond the FTC's notice-and-choice regime, what comes next? As a threshold matter, we need to diagnose the problem. What type of equilibrium are we in? One in which disclosure is consistent with consumer preferences, or something more akin to a lemons market that leads to suboptimal levels of privacy? That is, does privacy even want to unravel?

If the unmet condition preventing unraveling is lack of consumer demand, any intervention designed to promote credible disclosure is wasteful. This is because consumers are willing to pay for the additional information only if the value of the difference between the choices made with and without disclosure is greater than the cost of requiring that disclosure. If the choices are the same in both disclosure regimes, there can be no gain from disclosure. On the other hand, if research suggests that asymmetric information is the culprit, there is a more plausible case for some sort of consumer protection intervention to promote unraveling. For example, it might be that despite consumer demands for more privacy and firms' willingness to supply it, firms cannot convince consumers that they will actually follow through on their promises.

One possible intervention path is prescriptive and proscriptive regulation. For instance, in addition to mandated disclosures about information collection, government could provide baseline privacy standards. This approach could include mandates like data minimization and privacy by design, loyalty duties for data handlers, and bans on certain types of collection and use all together. The American Data Privacy and Protection Act,[9] currently being considered by Congress, represents such an approach, as could a forthcoming FTC rule.[10] The tradeoffs involved in this type of regulation are well known: in exchange for certainty, one loses nuance, which can be quite costly when harms and benefits are felt heterogeneously. These problems are exacerbated to the extent that government policymakers have imperfect information, which is almost certainly the case in the domain of online privacy.

---

8. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022).

9. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

10. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022). The FTC's recent proposed modification of its Order against Facebook presents another means by which the FTC can regulate conduct, although regulation through order applies only to a single company, not an entire industry. Press Release, Fed. Trade Comm'n, FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (May 3, 2023), www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data [https://perma.cc/83XC-378C] [hereinafter *Facebook Youth Data Prohibition*].

A second and more flexible intervention path would be to try to address the failure of the underlying conditions needed for unraveling to occur. Accordingly, maybe it is not time to discard the FTC entirely but instead to provide it with tools to transform what consumers might perceive as cheap talk into credible privacy commitments. Chief among them would be the ability to levy penalties sufficient to deter deception over privacy. At the same time, the FTC should signal a willingness to allow good-faith attempts to make privacy information more understandable to consumers by not finding overly broad implied privacy claims in privacy-related marketing.

The remainder of this Essay is organized as follows. Part II appraises the status quo, first examining the FTC's approach under Section 5 and its limitations in promoting unraveling. It then next explores the extent to which privacy unraveling is occurring, and if not, which conditions for its occurrence are not being met. Part III compares regulation to more market-preserving replacements for the FTC. Part IV concludes by suggesting a cautious approach, with increased empirical study to determine whether the limited evidence of privacy unraveling is more consistent with a lemons market or efficient levels of disclosure given information costs and consumer demand for privacy.

II. APPRAISAL OF THE STATUS QUO

In this Part, I first briefly summarize how the FTC regulates privacy under its statutory mandate. I next evaluate the privacy equilibrium we are in by first describing the conditions that undergird the unraveling result and assessing the extent to which these conditions are likely to be met today.

A. FTC Enforcement

Over the past two decades, the FTC has found reason to believe that numerous firms have violated Section 5 by making express or implied representations about their data practices that were materially false or misleading to a significant minority of reasonable consumers. Early FTC actions centered on breaches of express promises related to the collection and use of consumer data were pleaded as deception.[11] As the Internet matured, so did the FTC's application of its power to address "unfair or deceptive acts or practices" ("UDAPs").[12] For example, the FTC began to focus on not only express promises but also

11. *See, e.g.*, GeoCities, 127 F.T.C. 94 (1999) (settling charges that the company's privacy policy misrepresented its actual information collection and usage practices).

12. 15 U.S.C. § 45.

implicit representations about privacy.[13] The FTC has also expanded the use of UDAP cases beyond deception, finding the collection and use of certain types of sensitive data without adequate consent to be an unfair practice.[14]

In theory, both deception and unfairness operate like a negligence standard in that they cover only conduct that is net harmful to consumers. For example, only statements that are likely to materially mislead a significant minority of reasonable consumers are considered deceptive under the FTC Act.[15] Similarly, for conduct to be unfair, it must be likely to cause substantial and unavoidable consumer injury without offsetting benefits.[16] But this tort-like approach suffers two important shortcomings in creating economy-wide privacy norms, both related to the FTC's remedial powers.

The most important shortcoming of using Section 5 to deter firms from engaging in net harmful privacy practices is a lack of effective

---

13. *See, e.g.*, Complaint for Civ. Penalties, Injunction, & Other Relief ¶¶ 21–26, United States v. Facebook, Inc., No. 1:19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf [https://perma.cc/2DYP-EPKS]; Decision and Order, Snapchat, Inc., FTC Docket No. C-4501 (May 8, 2014) https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf [https://perma.cc/UUH9-VQCH].

14. The FTC, however, has used unfairness theories sparingly in its privacy cases, in large part because substantial injury in the context of privacy may be difficult to show. Most injuries involving suspect data practices are subjective, involving disutility from dignitary affronts or loss of autonomy from unwanted observation. *See, e.g.*, Complaint for Civil Penalties & Other Relief, Google Inc., FTC Docket No. C-4336 (Aug. 9, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf [https://perma.cc/S3CK-YGHN]. The FTC's Unfairness Policy Statement explicitly states that substantial consumer injury is unlikely to be satisfied by emotional or other subjective harms. Letter from Michael Pertschuk et. al., Comm'rs, FTC, to Wendell H. Ford & John C. Danforth, U.S. Sens., Consumer Subcomm. of Comm. on Com., Sci., and Transp. (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness [https://perma.cc/4QB5-FGLW] ("The Commission is not concerned with trivial or merely speculative harms . . . . Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."). To surmount this stricture, the FTC has leaned on potential physical and financial harms that can accompany surreptitious surveillance or unwanted publication of private data. *See, e.g.*, Complaint ¶ 19, DesignerWare, LLC, FTC Docket No. C-4390 (Sept. 25, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf [https://perma.cc/6UP6-3PSH] ("[C]onsumers are harmed by DesignerWare's unwarranted invasion into their homes and lives and its capture of the private details of individual and family life, including, for example, images of visitors, children, family interactions, partially undressed individuals, and couples engaged in intimate activities."). Recent cases against Kochava and BetterHelp involved the sharing of sensitive location and health data with third parties. FTC v. Kochava, Inc., No. 2:22-cv-00377-BLW, 2023 WL 3249809 (D. Idaho 2023); Complaint, BetterHelp, Inc., FTC Docket No. 2023169 (Mar. 2, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023169-betterhelp-complaint_.pdf [https://perma.cc/2UJ3-XGYT].

15. FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION 3 n.20 (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/Z7XN-A3HT].

16. FED. TRADE COMM'N, FTC POLICY STATEMENT ON UNFAIRNESS (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness [https://perma.cc/2QCX-7V2Z].

monetary remedies. Harm-based remedies can be used to effect optimal deterrence: if firms realize that they will be forced to pay for the harm their practices cause, they will engage only in acts that create more good than harm for society.[17] Clear lies will always fail this test.

Unfortunately, the monetary remedies available to the Commission for unfair or deceptive data practices are unlikely to create the needed internalization of consumer harm. If the FTC brings a case administratively, it can obtain only injunctive relief — requiring the firm to stop engaging in the challenged business practice and, in some instances, requiring the firm to take additional prophylactic measures.[18] These injunctive requirements, which typically run for twenty years, probably place non-trivial costs on defendant firms — especially if they require major changes in business models or reduce the ability to monetize consumer data.[19] But there is no correspondence between these compliance costs and consumer harm, which is a necessary condition to force firms to internalize the expected harm caused by their data practices.[20]

---

17. *See* Cooper et al., *Equitable Monetary Relief*, *supra* note 6.

18. In some cases, the FTC will include so-called fencing-in relief that prohibits conduct not alleged to have violated the FTC Act. *See, e.g.*, Telebrands Corp. v. FTC, 457 F.3d 354, 357 n.5 (4th Cir. 2006); FTC v. Colgate-Palmolive Co., 380 U.S. 374, 394–95 (1965). For example, the FTC has required, in an order, certain defendants to obtain "affirmative express consent" from their users before changing their data collection practices, although not alleging that failure to obtain opt-in consent had violated the FTC Act. *Compare* Decision and Order § II, Facebook, Inc., FTC Docket No. C-4365 (Aug. 10, 2012) (requiring Facebook to obtain "affirmative express consent" before using data in a materially different way), *with* Complaint ¶ 29, Facebook, Inc., FTC Docket No. C-4365 (Nov. 29, 2011) (arguing that failure to obtain "informed consent" for material changes to use of already collected data was an unfair practice). The FTC recently announced that it intended to modify its order against Facebook to prevent it from monetizing personal data from any user under the age of eighteen. *Facebook Youth Data Prohibition*, *supra* note 10.

19. Restrictions that reduce the ability to monetize data and subject the firm to the risk of substantial monetary penalties additionally may chill venture capital investment in tech startups. *See* John M. Wingate, *The New Economania: Consumer Privacy, Bankruptcy, and Venture Capital at Odds in the Internet Marketplace*, 9 GEO. MASON L. REV. 895, 915–18 (2001).

20. Section 19 of the FTC Act provides the Commission with the ability to obtain equitable relief and damages from companies after a fully litigated administrative proceeding, and only for conduct that a "reasonable [person] would have known . . . was dishonest or fraudulent." 15 U.S.C. § 57b. These conditions are unlikely to be satisfied for privacy cases, as to date, all cases have either settled or been brought in federal district court. Further allegations contained in the complaints involve misfeasance or failure to adequately disclose data practices, which may not rise to the level of "dishonest or fraudulent" conduct needed to satisfy Section 19. What is more, even if a case were to satisfy the Section 19 predicates, the subjective nature of privacy harms likely would make it difficult for the FTC adequately to quantify damages. For a discussion on potential measures to force a firm to internalize harm from data practices, see James C. Cooper & Bruce H. Kobayashi, *Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem*, 28 MICH. TECH. L. REV. 257 (2022). Nonetheless, the FTC recently has managed to obtain monetary settlements from two firms for administrative complaints that alleged unfair and deceptive data practices. Although there is no mention in the Order or other public statement, the monetary settlement is likely to avoid the cost of an administrative trial and potentially the threat of a subsequent Section 19 action. *See* Decision and Order, Avast Ltd. (Feb. 22, 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/D%26O-Avast.pdf [https://perma.cc/8DJ5-ZTUU] (requiring a payment of $16.5 million); Final

Although the recent *AMG Cap. Mgmt., LLC v. FTC*[21] decision has had important ramifications for the FTC's ability to remedy fraud-related to the sale of goods and services,[22] it is unlikely to have much of an impact on the FTC's privacy portfolio. The Commission's pre-*AMG* power to obtain equitable monetary relief was limited to recovering money that consumers spent on fraudulently marketed products.[23] The Commission's typical privacy case, however, does not involve monetary flows from consumers to the defendant firm, so there is no equitable monetary relief to obtain in the first place.[24]

Finally, the FTC can obtain monetary remedies for privacy violations against firms that have agreed to a consent order to settle Section 5 charges. Failing to comply with an order can be expensive — over $44,000 per violation — and the FTC has obtained substantial penalties against Google and Facebook for order violations.[25] The ability to obtain civil penalties for order violations may be effective at securing specific deterrence, but because this remedial power is limited to specific practices from which individual companies have agreed to abstain, it is unlikely to have a major impact on general deterrence.[26]

Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 14, 2023) https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf [https://perma.cc/9P34-L22S] (requiring a payment of $7.8 million).

21. 141 S. Ct. 1341 (2021) (holding that the FTC lacks authority to seek equitable monetary relief in federal court under Section 13(b) of the FTC Act).

22. *Id.* at 1344, 1347–49.

23. *See, e.g.*, FTC v. Commerce Planet, Inc., 878 F. Supp. 2d 1048, 1088–90 (C.D. Cal. 2012), *aff'd in part*, 642 F. App'x 680 (9th Cir. 2016), and *aff'd in part, vacated in part, remanded*, 815 F.3d 593 (9th Cir. 2016).

24. For example, most of the FTC's privacy cases involved free online services. *See* James C. Cooper, *Privacy Rulemaking at the FTC* at 231–33; notes 18–24 and accompanying text, in RULEMAKING AUTHORITY OF THE US FEDERAL TRADE COMMISSION (Daniel A. Crane ed., 2022). Only three cases have settled with any monetary remedies. *VIZIO* was brought in federal district court with the New Jersey Attorney General. $1.5 million of the $2.2 million total monetary remedy was paid to the FTC. *See* Fed. Trade Comm'n, Press Release, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent, FTC (Feb. 6, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million [https://perma.cc/Z3R4-S6XM]. The ability to obtain a monetary settlement may have rested on the fact that, unlike most privacy cases, *VIZIO* involved consumer expenditures on a product, which could be refunded. The FTC additionally has obtained monetary settlements for two administrative privacy cases. *See* Avast Ltd., *supra* note 20; BetterHelp, Inc., *supra* note 20.

25. *See, e.g.*, Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief at 3–4, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. Jul. 24, 2019) (ordering a $5 billion civil penalty); Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 2, 9, United States v. Google, Inc., No. CV 12-04177 (N.D. Cal. Nov. 16, 2012) (approving a $22.5 million civil penalty).

26. Order provisions can map out how the Commission intends to approach enforcement decisions. But the impact of an order provision on general deterrence is likely to be minimal, given that it is backed only by the possibility of initiating an administrative action, which, despite the concomitant costs, is less than civil penalties. The FTC Act also allows the Commission to seek civil penalties from any firm that engages in conduct that the FTC previously has found to be "unfair or deceptive" in a fully litigated administrative action against another

The second shortcoming of the current approach is due to difficulties in using Section 5 enforcement to create economy-wide rules that prohibit or prescribe certain data practices. First, consent orders — which comprise all but one of the FTC's privacy cases — are private agreements between the settling firm and the FTC.[27] As such, consent orders include a mix of corrective injunctions and fencing in that were produced in negotiations and apply only to the defendant's conduct; they do not define Section 5's requirements for the market as a whole. Further, while the FTC can obtain cease-and-desist orders in administrative and federal court actions, these injunctions must be tied to the allegedly unlawful conduct.[28] For example, if an FTC complaint alleges deception against an app for lying about tracking consumers despite expressly or implicitly representing it does not, an FTC order can require the firm to stop lying about tracking but not to stop tracking altogether.[29] Thus, a company can resolve the FTC's complaint by continuing to track as long as it is no longer deceiving consumers about the practice — which could include no longer making *any* express or implied representations about the presence or absence of cookies.[30]

The FTC can obtain changes in conduct only when it alleges that a firm's data practice is unfair. However, as discussed above, the FTC

---

firm, but only if the defendant had "actual knowledge" that their conduct of the prior case and their conduct was the same. 15 U.S.C. § 45(m)(1)(B); *see also* United States v. Hopkins Dodge, Inc., 849 F.2d 311 (8th Cir. 1988).

27. *See* 16 C.F.R. §§ 2.31–2.34.

28. *See Telebrands Corp. v. FTC*, 457 F.3d 354, 358 (4th Cir. 2006) (explaining that the FTC remedial order must bear a "reasonable relationship" to the underlying violation of Section 5).

29. *See, e.g.*, Decision and Order at 2, Nomi Technologies, Inc., FTC Docket No. C-4538 (Sept. 3, 2015).

30. Commissioners Ohlhausen and Wright both make this point in their respective dissents in *Nomi*. MAUREEN K. OHLHAUSEN, DISSENTING STATEMENT OF COMMISSIONER MAUREEN K. OHLHAUSEN IN THE MATTER OF NOMI TECHNOLOGIES, INC. 2 (2015), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-nomi-technologies-inc [https://perma.cc/6YLF-ZNTW]; JOSHUA D. WRIGHT, DISSENTING STATEMENT OF COMMISSIONER JOSHUA D. WRIGHT IN THE MATTER OF NOMI TECHNOLOGIES, INC. 4 (2015), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-joshua-d-wright-matter-nomi-technologies-inc [https://perma.cc/8AFD-3A2X]. The FTC can allege that failure to disclose a practice constitutes a deceptive omission, but this cause of action is limited to instances in which the data practice at issue would be so contrary to reasonable consumer expectations as to change the character of the product. For example, failing to disclose that a car is incapable of reaching highway speeds would be a deceptive omission. *See* Int'l Harvester Co., 104 F.T.C. 949, 1045 n.29 (1984); MAUREEN K. OHLHAUSEN, STATEMENT OF ACTING CHAIRMAN MAUREEN K. OHLHAUSEN IN THE MATTER OF LENOVO, INC. 1–2 (2017). A deceptive omission — a setting in which the defendant has made no representation at all — is distinct from a failure to adequately disclose a material fact that is necessary to prevent an express or implied claim from being misleading. For example, a representation that a website will collect "browsing history" may be deceptive if the website fails to adequately disclose that it will also be collecting sensitive health or financial information that users input into websites they visit. *See* Complaint ¶¶ 12–14, Sears Holdings Mgmt. Corp., FTC Docket No. C-4264 (June 4, 2009).

has sparingly used unfairness in its privacy cases due to the subjectivity associated with privacy harms. Further, because the FTC lacks the power to declare a data practice per se unlawful under its UDAP enforcement power, a firm typically can comply with an order preventing future unfair conduct by obtaining some form of heightened consent for the practice.[31] The FTC can use administrative or federal court litigation to establish privacy norms in Commission or appellate court precedent, respectively, but to date, the FTC has litigated only one privacy case.[32] Left is what some have called the FTC's "common law of privacy," which comprises the combination of reports and consent orders that map out what the FTC considers unfair or deceptive data practices in this space.[33] But regardless of the imperatives one can divine from past FTC enforcement decisions, their ability to control firm behavior exists in the shadow of the law — that is, the force of this soft law is ultimately a function of how seriously courts would take the FTC's legal theories.

B. Is Privacy Unraveling?

To move beyond the FTC, we need to know two things: the extent to which privacy may be unraveling under the status quo and, if it is not, why? The answer to these two questions will help us understand how much needs to be fixed and how best to do it. Before we answer these questions, it is necessary to first explain unraveling and the conditions needed to make it work.

1. Unraveling Explained

The concept of unraveling is straightforward. Imagine a market in which firms are ranked on a dimension of quality, such as safety, giving rise to a distribution. It is clear that the firm with the highest quality has an incentive to disclose this fact to attract customers from its rivals. But

31. *See, e.g.*, Decision and Order at 4, Facebook, Inc., FTC Docket No. C-4365 (Aug. 10, 2012). *But see, e.g.*, Decision and Order at 7, BetterHelp, Inc., FTC Docket No. C-4796 (July 14, 2023) (prohibiting the use of data for advertising regardless of consent).

32. The court originally dismissed the FTC's complaint for failure to sufficiently allege consumer injury. *See* FTC v. Kochava, Inc., 671 F. Supp. 3d 1161, 1171–77 (D. Idaho 2023). The FTC's amended complaint with more detailed allegations on harm survived dismissal.

33. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L.. REV. 583 (2014). An example of the FTC's use of consent orders to create law can be seen in a recent statement accompanying the settlement of its case against Avast Ltd., which explains how a series of recent settlements maps out the proposition that "sensitive data triggers heighted privacy obligations and a default presumption against its sharing or sale." FED. TRADE COMM'N, STATEMENT OF CHAIR LINA M. KHAN JOINED BY COMMISSIONER REBECCA KELLY SLAUGHTER AND COMMISSIONER ALVARO M. BEDOYA, IN THE MATTER OF AVAST LTD., COMM. FILE NO. 202-3033 2 (2024). The statement further notes that the FTC defines sensitive data that triggers these obligations to include "precise geolocation data," "biometric data," "health information," and "browsing records." *See id.*

this is not the end of the process — once the highest-quality firm has disclosed, the second-highest quality firm has an incentive to disclose its quality level, lest consumers assume that its quality is no higher than the remaining non-disclosing firms. Once the second-highest firm has disclosed, the third-highest firm finds itself facing the same dilemma and decides to disclose its quality. This process continues until all but the lowest-quality firm have disclosed their quality levels. Key to this result is what consumers infer from a failure to disclose: in equilibrium, silence is equivalent to reporting the lowest quality.[34] The upshot is that there should be a positive relationship between quality and incentives to disclose — indeed, all but the lowest-quality firms have strong private incentives to report their quality levels without government compulsion.

Unraveling benefits consumers in two main ways. First, the disclosure of previously hidden information allows consumers to sort vertically — along well-defined quality dimensions — and horizontally — according to idiosyncratic preferences. Second, to the extent that consumers respond to the new information, such as by allowing higher-quality firms to serve more customers or charge higher prices, firms will compete on this dimension. One study, for example, finds that once the FDA allowed firms to advertise the health benefits of high-fiber diets, consumers began to increase consumption of high-fiber cereals, and firms began to enter the market to provide new high-fiber formulations.[35]

While it is hard to deny the elegance of the unraveling result, its purest form rests on a variety of assumptions. This may explain why although the comparative statics of the unraveling model tend to hold — in that firms with lower disclosure costs and higher quality products are more likely to disclose[36] — most studies find less than full unraveling.[37]

On the demand side, for unraveling to work, consumers must reward firms for higher quality in the relevant dimension. For example, for car makers to tout safety, consumers must be willing to pay more for a safer car, ceteris paribus. Consumers also must make rational inferences about product quality from non-disclosure. If consumers fail

34. *See supra* note 1.

35. *See generally* Pauline M. Ippolito & Alan D. Mathios, *Information, Advertising and Health Choices: A Study of the Cereal Market*, 21 RAND J. ECON. 459 (1990).

36. David Dranove & Ginger Zhe Jin, *Quality Disclosure and Certification: Theory and Practice*, 48 J. ECON. LIT. 935, 951 (2010); *see, e.g.*, Alan D. Mathios, *The Impact of Mandatory Disclosure Laws on Product Choices: An Analysis of the Salad Dressing Market*, 43 J.L. & ECON. 651 (2000) (finding only partial unraveling for fat content in salad dressing); David Butler & Daniel Read, *Unraveling Theory: Strategic (Non-) Disclosure of Online Ratings*, 12 GAMES 73 (2021) (finding evidence of partial unraveling for hotels); Ippolito et al., *supra* note 35 (finding evidence to support unraveling for fiber content in the breakfast cereal market).

37. *See* Dranove et al., *supra* note 36, at 943, 950–51.

to understand the strategic nature of the revelation decision — that relatively high-quality firms have very little incentive to remain silent about a salient dimension of quality when reporting costs are low — they may overestimate the quality of non-reporting firms. Recent experimental work by Jin et al., for example, finds evidence consistent with unraveling theory for the highest-quality sellers but that intermediate-quality sellers fail to disclose due to beliefs that buyers will overestimate the quality of non-disclosing sellers.[38] Sellers' conjectures turn out to be correct, as the authors find evidence that consumers in the study are naïve, in the sense that they do not fully understand the strategic implications of a seller's decision not to disclose.[39]

On the supply side, sellers must know their quality level and the distribution of available quality; otherwise, they will not know where they fall in the distribution and therefore whether reporting will be beneficial. For example, recent research finds evidence that the lack of voluntary disclosure of energy audits by home sellers is due to uncertainty about the relative energy efficiency of their homes.[40] Although consumers have superior knowledge about their houses' energy consumption, they do not know how much energy their neighbor uses.[41] The extent to which firms disclose is also positively related to the cost of disclosure. Obviously, the more expensive it is to make quality claims understandable to consumers, the less likely sellers are to make them. Relatedly, if a seller cannot credibly commit to supplying the quality they promise, consumers will not respond.[42] Legal fines and reputational bonds can lend credibility by providing a punishment mechanism, but if the probability that a lie is detected is low, the expected punishment will be low even for a high punishment level.

2. The Evidence

Ultimately, the extent to which firms report to consumers how they collect and use consumer information is an empirical question. Addressing this question in a rigorous way is beyond the scope of this Essay, but casual empiricism suggests that privacy does not play a key role in most marketing campaigns. For example, a search on three

---

38. Ginger Zhe Jin, Michael Luca & Daniel J. Martin, *Is No News (Perceived as) Bad News?,* 13 AM. ECON. J. MICRO 141, 142–43 (2021).

39. *Id.*; *see also* Ginger Zhe Jin, Michael Luca & Daniel J. Martin, *Complex Disclosure*, 68 MGMT. SCI. 3236 (2022) (finding experimental evidence that sellers with intermediate qualities tend to send obscure rather than simple disclosures based on a belief — which is confirmed — that consumers will not punish them).

40. Erica Myers, Steven L. Puller & Jeremy West, *Mandatory Energy Efficiency Disclosure in Housing Markets*, 14 AM. ECON. J.: ECON. POL'Y 453, 483 (2022).

41. *Id.* at 476–77, 483.

42. *See* George Akerlof, *The Market for Lemons: Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 494 (1970).

online databases of national television and digital advertisements finds only a handful of advertisements reference privacy.[43] Further, there are ways, apart from marketing, that firms can employ to make their data policies salient to consumers, such as certifying compliance with a privacy standard — a way that originally was seen as a promise for promoting online privacy. Yet, one study finds that only twenty-seven percent of the sampled privacy policies claim compliance with some type of certification standard, such as Privacy Shield.[44] Certifications may not have worked because consumers may not have been familiar with the certifying organization, or consumers may have been rationally concerned about the incentives of for-profit certifiers. For example, research finds that websites with seals from TRUSTe, a private certification program, tended to have lower average privacy ratings than non-certified sites,[45] and the FTC brought an action against TRUSTe for misrepresenting their certification procedures.[46]

Although there is little evidence of widespread competition over privacy, it is not completely absent; there is some evidence that firms are making privacy claims for products where privacy might be an important dimension of quality. In the search engine market, for instance, DuckDuckGo — and, to a lesser extent, Bing — have advertised how they provide privacy superior to that of Google.[47] Further, WhatsApp

---

43. Apple, WhatsApp, Facebook, Sekur, and DuckDuckGo were the only online commercial companies that had advertisements mentioning privacy. The search also turned up ads for VPNs, Reputation Defender, and mail-order incontinence products. *See, e.g.*, ISPOT.TV, https://www.ispot.tv/search/privacy/ad [https://perma.cc/HKJ9-686H] (reporting the results from a search of television and online ads that mentioned the word "privacy").

44. *See* Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J. LEG. STUD. S13, S27 (2016) ("The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the United States Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce."); *Privacy Shield Framework*, DATA PRIV. FRAMEWORK PROGRAM, https://www.privacyshield.gov/welcome [https://perma.cc/SRX8-DHAJ]. The Department of Commerce administered the framework through its statutory authority to foster, promote, and develop international commerce. 15 U.S.C. § 1512. A new US-EU data protection framework is in negotiations to replace Privacy Shield, following Privacy Shield's repudiation in 2020 by the Court of Justice of the EU, as well as the recent ruling against Meta for General Data Protection Regulation ("GDPR") violations by the Irish data protection authority. Thibaut D'hulst, *Irish Data Protection Authority Suspends Meta's EU-US Transfers, Imposes €1.2 Billion GDPR Fine*, LEXOLOGY (June 12, 2023), https://www.lexology.com/library/detail.aspx?g=74e9efe3-ac47-4352-9639-32c0257d8f87 [https://perma.cc/C3GV-NJEC].

45. Benjamin Edelman, *Adverse Selection in Online Trust Markets*, 10 ELEC. COM. RES. & APPS. 17, 20 (2011); Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIV. L. 15, 25 (2015). These findings are consistent with adverse selection into certification, where sites that have established reputations for privacy not needing a third-party certifier.

46. Decision and Order, True Ultimate Standards Everywhere, Inc. (TRUSTe), FTC Docket No. C-4512 (Mar. 18, 2015).

47. DuckDuckGo shares have remained stagnant despite these efforts to make their privacy. For example, DuckDuckGo increased its advertising spending by over eighty percent

has recently engaged in a media campaign promoting privacy as a core feature.[48] There is also evidence of privacy unraveling for mobile platforms. In an effort to distinguish itself from the Android ecosystem, Apple has made privacy a centerpiece of its brand in recent years, advertising its encrypted chat and cloud storage features, in addition to its recent app store tracking consent requirements.[49] Further, online therapy service BetterHelp made privacy a centerpiece of its advertising — claims that the FTC challenged as false.[50] Finally, one study finds evidence that adult websites tend to make their policies regarding anonymity of visitors relatively more salient to consumers than they make other terms and that cloud computing sites tout their data security practices.[51]

C. Which Equilibrium Are We In?

Although privacy advertising is not completely absent, it is far from ubiquitous. If data is the price we pay to access myriad services, why do we see firms saying far less about privacy than they do about price — or most other attributes, for that matter? Before we pronounce the meager evidence of unraveling as a symptom of a market failure, however, we need further investigation. We need to know which equilibrium we are in: one in which disclosure is consistent with consumer preferences; a lemons market in which asymmetric information plagues consumers and firms and keeps them from the privacy they want; or something in between. That is, we need to know if privacy even wants to unravel.

If it does not, any intervention to force a new equilibrium will be socially wasteful. If it does, any intervention must improve upon the status quo. The problem in designing policies is distinguishing between the effects of asymmetric information and lack of consumer demand,

---

in recent years, yet its market share has continued to hover around 2.5%. *See* Max Willens, *'They're Primed': DuckDuckGo Wants to Be 'the Easy Button' for Privacy on the Internet. Do Internet Users Want One?*, DIGIDAY (Jan. 11, 2022), https://digiday.com/media/theyre-primed-duckduckgo-wants-to-be-the-easy-button-for-privacy-on-the-internet-do-internet-users-want-one/ [https://perma.cc/CAC9-G7X6]; *Search Engine Market Share United States of America*, STATCOUNTER, https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america [https://perma.cc/XY7X-TG73]; *see also* Danny Sullivan, *Is Microsoft's Scroogled Campaign Working? Not if Gaining Consumers is the Goal*, MKTG. LAND (Oct. 16, 2013), https://martech.org/microsoft-scroogled-campaign [https://perma.cc/DQN5-NJ73]. However, there is little evidence that these efforts have impacted consumer behavior. *See* Cooper et al., *Antitrust and Privacy*, *supra* note 4, at 358–61.

48. *WhatsApp TV Spot, 'A New Era of Privacy*,' ISPOT.TV (Oct. 17, 2022), https://www.ispot.tv/ad/25bs/whatsapp-a-new-era-of-privacy [https://perma.cc/89ZT-CVLD].

49. The Ninth Circuit recently recognized this type of positioning over privacy as a procompetitive justification in a monopolization case. Epic Games, Inc. v. Apple, Inc., No. 21-16506, 2023 WL 3050076, at *21–23 (9th Cir. 2023).

50. *See supra* note 31.

51. *See* Marotta-Wurgler, *supra* note 44, at S31–S35.

because they look the same. If consumers are not likely to respond to privacy commitments even if perfectly comprehensible and enforceable, firms rationally will not provide this information, and no amount of forced disclosure will change privacy levels. Conversely, if the market for privacy suffers from adverse selection because firms cannot credibly commit to consumer-friendly data practices, or if firms lack knowledge about how their data practices fit in the distribution, fixing the informational environment could help privacy unravel.

1. Lack of Demand

On one hand, the extent to which consumers reward firms that provide higher levels of privacy is uncertain. Ceteris paribus, most consumers prefer more privacy to less.[52] But if privacy is negatively correlated with other quality dimensions — for instance, if data collection and use enable personalization or enhanced monetization from tailored advertisements leads developers to provide richer content and features at lower prices — consumer demand may not respond to increases in privacy.[53] In this manner, the lack of privacy unraveling may merely reflect rational consumer choice in the face of opportunity costs.[54]

Consistent with this view, one experiment finds that in a sample of Gmail users who are educated about Google's privacy policy (and uniformly agree that it is privacy invasive), only thirty-five percent would be willing to pay at all for a version of Gmail that did not use email

52. *See* Tesary Lin, *Valuing Intrinsic and Instrumental Preferences for Privacy*, 41 MKTG. SCI. 663 (2022) (explaining and documenting with experimental evidence consumers' intrinsic value of privacy).

53. *See, e.g.*, Cooper et al., *Antitrust & Privacy*, *supra* note 4 (finding a robust negative association between an app's privacy grade and its user rating). For empirical work finding a positive relationship between monetization and the quantity and quality of content see, for example, Benjamin Shiller, Joel Waldfogel & Johnny Ryan, *The Effect of Ad Blocking on Website Traffic & Quality*, 49 RAND J. ECON. 43, 51–58 (2018), and Garrett A. Johnson, Tesary Lin, James C. Cooper & Liang Zhong, *COPPAcalypse? The YouTube Settlement's Impact on Kids Content* (May 1, 2023) (unpublished manuscript), https://ssrn.com/abstract=4430334 [https://perma.cc/3WVL-2DRC].

54. Where this negative correlation between privacy and content exists, it lends itself to horizontal rather than vertical sorting, in the sense that consumers choose the combination of privacy and quality on other dimensions based on their idiosyncratic preferences for both. To the extent that we fail to observe firms making credible claims about enjoying a high-privacy position on this horizontal continuum but high-quality claims are ubiquitous, it suggests that there may not be a large demand for the high privacy/lower quality position. Relatedly, to the extent that consumers feel that there is sufficient information about them in the hands of third parties to make accurate classifications about what they perceive to be sensitive attributes (e.g., sexual preferences or political leanings), they may perceive the marginal privacy cost of revealing additional information to be quite small. Of course, current data both reveals information about current behavior and can predict personal attributes. Thus, the extent to which such perceptions are widely held will depend on how consumers view the privacy implications of current observation versus the use of current observation to predict relatively unchanging characteristics.

content analysis to serve ads, and of this minority, the median willingness to pay was $15.[55] Relatedly, a recent field experiment shows that sophisticated undergraduate students were willing to trade personal information when presented with small incentives to reveal this information, a result that held regardless of a student's stated privacy preferences.[56] Similarly, experimental research in the lab and the field generally finds that consumers are willing to pay only a small amount to avoid the collection and use of various types of personal information (or willing to accept relatively small amounts of money to relinquish their personal information) in the typical online context.[57] Although this body of empirical work does not directly measure consumers' willingness to trade personal information for access to online content or services, it does suggest that, unless the value of online content is quite small, most consumers would be likely to make this trade.

Taken as a whole, the empirical and experimental evidence suggest that when faced with a tradeoff, consumers tend to choose other product dimensions (e.g., lower price, better functionality) over enhanced privacy protection. To the extent that these decisions are rational and informed, the relative paucity of firms making privacy claims is consistent with consumer preferences.

2. Informational Problems

On the other hand, there are a host of informational problems for both consumers and sellers that may limit the potential for privacy to unravel. As noted, if informational asymmetries render privacy promises credence goods, sellers may have difficulty convincing consumers that their privacy claims are not lies. While making privacy claims may not be any more costly than making other claims, the ability to credibly commit to these claims is where the difficulty likely arises.[58] First, even apart from undecipherable privacy policies, consumers may have

---

55. Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. LEGAL STUD. S69, S77–80 (2016).

56. Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* 8–14 (Nat'l Bureau of Econ. Rsch., Working Paper No. 23488, 2017). Although this experiment does not involve a trade of privacy for service directly, it does suggest that consumers are willing to trade privacy to acquire relatively low-value items (in this case, a pizza). *Id.*

57. *See* Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 479 (2016); Jeffrey T. Prince & Scott Wallsten, *How Much is Privacy Worth Around the World and Across Platforms?* 31 J. ECON. MGMT. & STRATEGY 841, 852–53 (2022) (using a discrete choice experiment and finding that, on average, American consumers are only willing to pay a monthly fee of $1.82 to avoid location tracking and $3.75 for browsing across different platforms); Scott J. Savage & Donald M. Waldman, *Privacy Tradeoffs in Smartphone Applications*, 137 ECON. LETTERS 171, 173–74 (2015) (employing similar methodology and arriving at similar findings).

58. *See, e.g.*, Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEG. F. 95, 156 (2013).

difficulty evaluating even a straightforward privacy promise in marketing. For example, when a company says it will not sell consumer data, does this include sharing data with third-party analytic firms or advertisement networks? More importantly, all but the most tech-savvy consumers have no way of verifying that a company is adhering to their promise to, for example, remove trackers from emails before sending them to their inboxes.[59] And while public or private enforcement against companies that lie about privacy can help make representations credible, lack of detection coupled with standing issues for private plaintiffs and the FTC's lack of monetary remedies means that many lies likely go unpunished.[60] In the end, if firms cannot convince consumers of the veracity of their privacy claims, firms will see no point in providing high privacy, and rational consumer expectations in the face of asymmetric information become a self-fulfilling prophecy.

Moreover, firms may also lack information about their own data practices and where they fit on a continuum of data practices, which mutes incentives to report. In the context of privacy, firms may not fully appreciate the consumer impact of their data practices, and, even more likely, may not understand where their practices fit in the distribution of possible data practices. If this is the case, beyond the dense legalese found in privacy policies, firms may be hesitant to make their data practices salient for fear that it will put them at a competitive disadvantage or subject them to a suit for deception.

Relatedly, even if a firm believes correctly that it has better-than-average data practices and thus would benefit from disclosing, it must also consider the potential that consumers do not understand the full distribution of potential harms. Thus, disclosure — while highlighting a firm's relatively better data practices — risks causing consumers to place less value on all products in the market (including the disclosing firm's), because they now perceive the entire distribution of possible qualities as lower than before the disclosure. For example, a credit card firm that touts its data security practices against hackers might cause consumers to believe that all credit cards are inherently riskier than cash, even if the disclosing firm has superior security relative to its credit card competitors.

Finally, the current enforcement regime could play a role in firms' willingness to market their privacy practices. For example, firms may be worried about providing general commitments in marketing for fear of liability for deception if a broad claim about privacy could be seen

---

59. *DuckDuckGo TV Spot, 'Watching You: More Email Privacy*,*'* ISPOT.TV (Sept. 26, 2022), https://www.ispot.tv/ad/2Z5D/duckduckgo-watching-you-more-privacy [https://perma.cc/T5ZM-H5KE].

60. For example, one study finds that that the terms of most privacy policies that claim adherence to third-party guidelines do not actually comply. *See* Marotta-Wurgler, *supra* note 44.

as making specific implied claims that may not be true. For example, suppose a social media app adopted a policy that it would not track users to serve targeted ads but provided certain hashed consumer information to third-party analytic firms to improve its website. A general statement touting its privacy commitments could lead to liability if an enforcer (or a private party acting under a state UDAP law) found that the representation led to an implied claim that the site did not share data with any third parties.[61] Perhaps this is one reason why firms rely on privacy policies, where details can be spelled out expressly (even if incomprehensibly) without fear of liability for implied claims that a significant minority of reasonable consumers may take away.

* * * * *

At the end of the day, the sparse evidence of unraveling could be due to lack of adequate consumer demand for enhanced privacy; lack of information about the distribution of privacy practices; the inability of firms to commit to policies; or perhaps some combination of all three. The problem is that each of these explanations predicts the same observed outcome. Before we cast aside the FTC's current approach and replace it with something else, we need empirical evidence to help us understand what is causing what we see in the marketplace. We need an identification strategy. Without the correct diagnosis, we cannot prescribe the correct treatment, which might include maintaining the status quo.

While it is certainly beyond the scope of this Essay to spell out such a research agenda, viable empirical paths might include both experimental and field research. For example, in an experimental setting, one might see if consumers exposed to advertisements touting different levels of privacy actually understand the ads as making differential privacy claims. Further, empirical work should examine the extent to which claims of superior privacy — even if understood properly — are

61. This hypothetical is not fanciful. For example, Apple is facing class action suits for allegedly deceiving consumers by, inter alia, touting privacy in its advertisements but collecting analytics data from its own apps. *See, e.g.*, Complaint ¶ 8, Libman v. Apple, Inc., No. 5:22-cv-07069 (N.D. Cal. Nov. 10, 2022); Complaint ¶ 1–14, Serrano v. Apple, Inc., No. 2:23-cv-00070 (E.D. Pa. Jan. 6, 2023). Similarly, DuckDuckGo faced scrutiny by the Better Business Bureau's National Advertising Division ("NAD") for potentially unsubstantiated privacy claims related to advertisements stating it does not share consumer data with third parties. *See National Advertising Division Finds Challenged DuckDuckGo Privacy Claims Supported; Recommends Clarifications for Use of App*, BETTER BUS. BUREAU NAT'L PROGRAMS (June 23, 2023), https://bbbprograms.org/media-center/dd/duckduckgo-privacy-claims [https://perma.cc/MK95-G74B] ("NAD examined DuckDuckGo's potentially overbroad online privacy protection claims, the accuracy of which consumers may not be able to assess on their own.").

material in that they alter consumers' purchase decisions.[62] In a field setting, one might examine whether consumers are more likely to believe firms that have more at stake when making privacy claims — that is, does the threat of punishment make their claims more credible? Ideally one could look for an exogenously imposed treatment — such as being put under FTC order for privacy violations — that increases the cost of lying for some firms but not others in the same industry.

III. IF NOT THE FTC, THEN WHAT?

If the data suggests that something other than lack of consumer demand is driving the lack of unraveling, there are two broad paths for moving beyond the FTC: embracing some form of proscriptive and prescriptive regulation or finding better ways to promote unraveling so that the market can provide the distribution of data practices that consumers demand. Below, I evaluate each approach.

A. Regulation

By regulation, I refer to prohibitions and requirements regarding the way that data can be collected and processed — that is, substantive standards as opposed to administrative requirements, such as reporting or disclosures. Regulations could take the form of "rules," such as a blanket ban on targeted ads served on content directed at kids, or standards, such as "data minimization" requirements or duties of loyalty.[63] A rules-based regime has the advantage of certainty and reducing enforcement costs; rather than having to prove that the defendant's conduct failed to meet a standard (e.g., deception or unfairness), the enforcer need only show that the conduct at issue was the same as that prohibited by the rule.[64] It is important to note that there is nothing inherently wrong with a regulatory approach as long as the regulator has accurate information about the relevant costs and benefits. When this assumption fails to hold, regulations typically suffer from two defects.

First, if regulators measure costs and benefits with error, the regulatory standard of care (which in the context of privacy would translate into how covered parties collect, process, and share data) will be stochastic and possibly biased, causing overdeterrence. When regulatory requirements are clear, there is a sharp reduction in expected costs at the standard, leading firms rationally to meet the standard to minimize the sum of accident and avoidance costs. But when regulatory requirements are ambiguous or subjective, firms risk being found in violation

62. One could also vary industries (e.g., search and sporting goods) and background government regulatory regimes (e.g., strict bans versus notice-and-choice).

63. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

64. *See* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 674–75 (D.C. Cir. 1973).

even if they meet or exceed the socially optimal level of care. Rationally, this causes firms to take more than optimal care — a result that holds even if the regulator sets the correct standard on average.[65] In the context of privacy regulation, for instance, this problem could arise when regulators or courts must determine whether a firm has complied with inherently subjective standards, such as data minimization or a duty of data loyalty.[66]

Second, what regulation gains in certainty and ease of enforcement, it loses in flexibility by treating all covered practices as if they have the same cost-benefit profile. Even if the standard of care is not stochastic, if a regulation is applied to a heterogenous population, there are welfare losses due to the fact that the rule requires too much care for some and too little care for others. The size of this loss is positively related to the variance of the relevant parameters in the affected population.

Take, for example, a blanket ban on tailored advertising based on any type of online tracking. No one seriously disputes that all else constant, consumers value their privacy. But holding the type of information collected constant, different people will suffer different privacy harms, because privacy sensitivity varies across individuals and contexts.[67] The same can be said on the benefit side. Firms monetize consumer data through a variety of mechanisms. For example, consumer data can be used to increase engagement and traffic or to target ads — which increases revenues from a given amount of traffic.[68] Note that

---

65. This result holds for most distributions that are not too dispersed. If the variance of the distribution of standards is quite large, it can lead to underdeterrence. *See* Richard Craswell & John E. Calfee, *Deterrence and Uncertain Legal Standards* 2 J.L. ECON. & ORG. 279 (1986); Steven Shavell, *A Model of the Optimal Use of Liability and Safety Regulation*, 15 RAND J. ECON. 271, 276–77 (1984). Large penalties and a distribution of standards biased toward too much care exacerbate this problem. *See* Cooper et al., *Equitable Monetary Relief*, *supra* note 6 (proposing reducing penalties as an optimal means to deal with a stochastic standard).

66. *See, e.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law* 104 B.U. L. REV. (forthcoming 2024) (manuscript at 44), https://ssrn.com/abstract=4333743 (proposing a duty of loyalty and a duty to avoid unreasonable risk for firms that obtain "murky" consent) (on file with author).

67. *See* Acquisti et al., *supra* note 57, at 446–47.

68. Several researchers have studied the impact of moving from targeted to contextual ads and found large reductions in publisher revenue as a result. *See, e.g.*, Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising,* 57 MGMT. SCI. 57, 57–58, 64 (2011) (sixty-five percent reduction in revenue); Howard Beales & Jeffrey A. Eisenach, An Empirical Analysis of the Value of Information Sharing in the Market for Online Content 11–13 (Jan. 2014) (unpublished manuscript), https://ssrn.com/abstract=2421405 (sixty-six percent reduction) [https://perma.cc/3UF9-MK79]; Garrett A. Johnson, Scott K. Shriver & Shaoyin Du, *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, 39 MKTG. SCI. 33, 34 (2020), (fifty-two percent reduction); Deepak Ravichandran & Nitish Korula, *Effect of Disabling Third-Party Cookies on Publisher Revenue*, GOOGLE (Aug. 27, 2019), https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf [https://perma.cc/J7GD-ZBLP] (sixty-four percent reduction); *The Value of Personalized Ads to a Thriving App Ecosystem*, FACEBOOK (June 18,

the monetization process typically requires that at least some consumers benefit from the data use — for example, more relevant advertising, better content, and more customization will be valuable to some consumers; otherwise firms would not expend resources to engage in these practices. As with the privacy harms, consumers will value these benefits differently. Ultimately, how data collection and use impacts individuals is likely to be highly complex and idiosyncratic, depending on the joint distribution of privacy harms and data collection benefits.[69] Given what is likely a highly dispersed distribution of costs and benefits associated with such a policy, it will supply the optimal amount of privacy for only a small part of the distribution, provide too much privacy for some, and provide too little privacy for others.[70] That rules are far less adaptable to rapidly changing harm and prevention costs only exacerbates this potential problem with rulemaking in a dynamic environment.[71]

B. Support for Unraveling

Regulation might be appropriate when (1) there is broad agreement that the conduct at issue is harmful and (2) the government has sufficient information to craft a correct standard.[72] For all other cases, it is

---

2020), https://developers.facebook.com/blog/post/2020/06/18/value-of-personalized-ads-thriving-app-ecosystem [https://perma.cc/L22W-WZZ5] (fifty percent reduction). There is also a host of empirical evidence suggesting that the elimination of targeted advertising reduces content. *See, e.g.*, Samuel G. Goldberg, Garrett A. Johnson & Scott K. Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR* 3, 33 (L. & Econ. Ctr. Geo. Mason Univ. Scalia L. Sch. Rsch. Paper Series No. 22-025, 2022), https://ssrn.com/abstract=3421731 [https://perma.cc/DG3C-3P6E]; Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from the GDPR* 24–27 (Nat'l Bureau Econ. Rsch., Working Paper No. 26900, 2020), https://www.nber.org/papers/w26900 [https://perma.cc/ZBA7-AJ6J]. The reduction in advertising revenue falls by (as statistically significant) twenty-five percent initially, but while the point estimate for the entire post-GDPR period suggests an economically significant decline (-16.8%), it is not statistically significant. *Id.* at 26–27. As the authors note, this is likely due to a gradual twelve percent increase in the average bid, likely due to the fact that post-GDPR observable consumers have more observable conversion rates. *Id.* at 25; s*ee also* Christian Peukert, Stefan Bechtold, Michail Batikas & Tobias Kretschmer, *Regulatory Spillovers and Data Governance: Evidence From the GDPR*, 41 MKTG. SCI. 746, 754–61 (2022) (finding substantial reductions in interactions with third-party data vendors after GDPR).

69. *See* Daniel P. O'Brien & Douglas Smith, *Privacy in Online Markets: A Welfare Analysis of Demand Rotations* (Fed. Trade Comm'n Bureau of Econ., Working Paper No. 323, 2014), https://www.ftc.gov/system/files/documents/reports/privacy-online-markets-welfare-analysis-demand-rotations/wp323.pdf [https://perma.cc/M6Y7-DFXG].

70. James C. Cooper, *Separation Anxiety*, 21 VA. J.L. & TECH. 1, 50–51 (2017).

71. A change to a rule requires using the notice-and-comment procedure. 5 U.S.C. § 553; 15 U.S.C. § 57a(a)–(b).

72. Under this standard, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code), and the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2000), may be approximately optimal to the extent that most consumers have strong preferences to keep information about their health and children private. *See*, *e.g.*, Lin, *supra* note

preferable to at least attempt a market allocation of data practices, which is what the FTC has attempted to do through its notice-and-choice regime. Assuming privacy wants to unravel, we should at least try to identify and potentially fix what is stopping it from doing so.

If the problem is information, one branch of this path might include some form of mandated disclosures. Standardized privacy disclosures could help consumers shop among firms.[73] Further, to the extent that firms underestimate where they stand in the distribution of privacy practices among their competitors, they may lack incentives to disclose. Standardized disclosure requirements could help unraveling along both of those dimensions.[74] At the same time, there is a large empirical literature suggesting that government-mandated disclosures are ineffective,[75] or at least not as effective as are market-based communications.[76] Further, for fear of having to disclose negative information to consumers, mandated disclosures can mute incentives for firms to discover the true nature of their products, which perversely can reduce the information available to consumers.[77] Thus, before considering any sort of mandated disclosure, there must be evidence that firms lack incentives to reveal relevant information voluntarily and, relatedly, that consumers actually value this information more than it costs to produce.

An alternative path to government-mandated disclosures is removing the impediments to unraveling and allowing firms to choose the messages that they believe will appeal to consumers' demands.[78] For consumers to believe firms' privacy claims, there must be some cost to lying. That is, lies about privacy must be detected and punished. Reputation often plays that role for most products: the lie is detected once

---

52, at 674–75 (finding that in experimental settings, consumers place the highest value on privacy regarding their children); Ravi Gupta, Raghuram Iyengar, Meghana Sharma, Carolyn C. Cannuscio, Raina M. Merchant, David A. Asch et al., *Consumer Views on Privacy Protections and Sharing of Personal Digital Health Information*, JAMA NETWORK OPEN, Mar. 2023, at 1 (examining consumers' willingness to share health information in different settings).

73. For example, firms may have incentives to obfuscate their true privacy practices to prevent consumers from shopping, and thus reduce effective competition.

74. Indeed, some studies have shown that health grades for hospitals and hygiene reports for restaurants have had some success in improving quality. *See* Dranove et al., *supra* note 36, at 952–55; *see also* Mathios, *supra* note 36 (finding evidence that mandated nutrition labeling reduced consumption of the highest-fat salad dressings).

75. *See, e.g.*, Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647 (2011).

76. *See, e.g.*, Ippolito et al., *supra* note 35; Mathios, *supra* note 36.

77. *See, e.g.*, Mitchell Polinksy & Steven Shavell, *Mandatory Versus Voluntary Disclosure of Product Risks*, 28 J.L. ECON. & ORG. 360, 361–62 (2012); Steven Shavell, *Acquisition and Disclosure of Information Prior to Sale*, 25 RAND J. ECON. 20, 21 (1994).

78. Indeed, research suggests that consumers are more responsive to firm than government communication about the health benefits from various dietary choices (e.g., high fiber or low fat). *See, e.g.*, Ippolito et al., *supra* note 35 (finding evidence to support unraveling on fiber content in the breakfast cereal market).

the product is used, and the punishment is a lack of repeat and new customers. But this mechanism works only when consumers can learn whether the claim was true after the fact, a condition that may not hold for privacy promises. Thus, a first step would be to provide an enforcement agency with the ability to levy harm-based penalties for deception. Consumer harm from deception comes from two sources: revenue from marginal consumers tricked into purchasing the product and any price premium paid by inframarginal consumers, who would have purchased the product without the deceptive marketing.[79] If firms are required to internalize this harm, they will have correct incentives with respect to privacy representations.[80] This model works well when consumers pay for a product, with the assumption that promised privacy is part of the bargain. However, as is the case with many online platforms, the explicit price is zero dollars When no money changes hands, a proxy remedy could be based on marginal revenue generated from marginal consumers — those lured to the platform by privacy promises.[81]

At the same time, the FTC could make it clear through speeches or a formal policy statement that it will not seek monetary remedies against firms that make good faith attempts to make simplified privacy claims. For example, a firm that claims not to share data with third parties should not be penalized if it uses a third party to perform analytics. If the FTC is too quick to find broad implied privacy claims from simple statements, then firms will be chilled from trying to make claims that consumers can understand. The upshot is that firms will instead relegate all privacy promises to the privacy policy — an outcome that almost guarantees less, rather than more, competition over privacy.

IV. CONCLUSION

Firms are not shy about disclosing their low prices to attract consumers but are relatively stoic when it comes to their data practices. If data is increasingly the "price we pay" to gain access to online content and services, this silence is surprising. Before we completely jettison the FTC's light-touch notice-and-choice approach for some form of rigid regulation, empirical study is needed to determine whether the reality we observe is the product of severe informational asymmetries or lack of consumer demand — that is, are we in a lemons market, or is the limited evidence of privacy unraveling consistent with efficient

79. *See* Cooper et al., *Equitable Monetary Relief*, *supra* note 6, at 665.

80. *Id.*

81. The economically efficient measure of damages would be the additional willingness to pay (beyond the services the platform provides) for the privacy promised for these marginal consumers, inflated by a multiplier to account for the fact that the probability of detection is less than one. Given the difficulty in this measurement, revenue from these consumers (again, inflated by a multiplier to account for imperfect detection) is an administrable proxy that will provide adequate deterrence against privacy lies. *Id.*

levels of disclosure given information costs and consumer demand for privacy relative to other dimensions of quality? Only after we know where we are can we determine the best path forward. We should give privacy a chance to unravel, but only if it wants to.