Before the

FEDERAL TRADE COMMISSION

Washington, D.C. 20580

Re: Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security

---

Comments of

The Program on Economics & Privacy

George Mason University, Antonin Scalia Law School

TechLaw

University of Arizona, James Rogers College of Law

November 21, 2022

1. Introduction and Summary

This comment is in response to the Federal Trade Commission's (FTC) Advance Notice of Proposed Rulemaking on "Commercial Surveillance and Data Security" (ANPR), which requests information "on the prevalence of commercial surveillance and data security practices that harm consumers."[1] We urge the Commission not to issue a proposed rule. There is insufficient reason to believe consumers suffer widespread harm from the collection and use of information that is routinely employed to customize and improve online content and services, including the use of tailored advertising.[2] At the same time, there is substantial empirical evidence to suggest that the collection and use of consumer data in commercial contexts provide substantial benefits. Accordingly, a broad rule of the type suggested in the ANPR is likely to do more harm than good, imposing substantial costs in return for meager benefits. The current case-by-case approach, which targets specific harmful practices, is far more appropriate for this setting.

This comment makes the following main points:

- Any rule that the FTC were to consider must address a *specific* act or practice that *harms* consumers, and that act or practice must be *prevalent*. These requirements oblige the FTC to demonstrate a causal link between a precisely defined practice and consumer injury, as well as evidence that these practices are widespread. Neither the FTC's numerous privacy settlements nor the extant empirical evidence provides the legally required support for a rule that would place *per se* restrictions—backed by potential civil penalties of over $46,000 per violation—on the collection and use of the type of consumer information that routinely goes into the type of personalization and zero price services that provide benefits to consumers, content creators, app developers, and other firms.

    - Although consumers clearly value privacy, they also value many other things provided to them free of charge—such as email, search, social media, video and audio streaming, and gaming—by an ad-supported online ecosystem made possible by the collection and use of consumer information. Given consumers' budget constraints and opportunity costs, it should not be surprising that we observe them allowing the collection and use of information about them in these contexts. This finding appears robust to most experimental and field settings.

[1] Fed. Trade Comm'n, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022). This comment responds most directly to Sections IV.a. and c (questions 4-6, 24-29, 41-43, and 62-63), although many points regarding the statutory prerequisites for a trade regulation rule and the need to conduct a benefit-cost analysis based on empirical evidence are germane to the entire ANPR.

[2] By collection and use of consumer data, we broadly refer to data derived from cross-site or cross-app persistent device identifiers, such as first- and third-party cookies, which are used to customize content and advertising, and for analytics involving metrics like engagement, conversions, and referrals. By tailored advertising, we refer to online programmatic advertising that allows advertiser to base their bids on user characteristics predicted with data from a variety of sources (including persistent device identifiers) as opposed to only the context of the website or app serving the impression.

- Restricting the ability of firms to use collect and use the type of consumer information necessary to engage in personalization will reduce value-creating voluntary exchanges that come from enhanced consumer information.

- Empirical analysis also suggests that consumers of ad-supported content can suffer– both in terms of reduced output and lower quality—when there are restrictions on the ability to engage in tailored advertising. Further, the ability to enter a market with an advertising-based model enhances competition.

- There are reasons to believe that consumers may lack complete information about data collection and use in these settings. Nonetheless, that personalization creates obvious benefits, coupled with observed consumer behavior and the rich extant empirical literature, makes the proposition that *per se* restrictions on the collection and use of data employed to make such personalization possible are needed to prevent "widespread" consumer harm highly dubious.

- As a threshold matter, the Commission lacks the legal authority to issue rules under its power to proscribe "unfair methods of competition." Further, while privacy regulation can negatively impact competition, neither theory nor empirical evidence suggests a relationship between a firm's market power and its privacy practices.

- Any proposed rule must consider First Amendment issues. A rule that burdens behavioral advertising has to survive intermediate scrutiny under the *Central Hudson* test, and any rule that burdens the collection of data for non-advertising purposes, or that burdens the use of data for purely expressive purposes, would have to survive even more searching scrutiny. A wholesale prohibition, based on speculative evidence of consumer harm, will not pass constitutional scrutiny.

- Finally, we urge the Commission to consider sound empirical evidence when considering whether to issue a proposed rule. The FTC's Bureau of Economics comprises approximately 80 of the world's leading consumer protection and competition economists, making the FTC extraordinarily well-positioned to produce its own empirical evidence and to evaluate the relevant extant empirical literature. Yet, the ANPR does not appear to consider any of the rich empirical literature that examines the tradeoffs between privacy regulation and various economic outcomes for consumers and firms. Instead, the ANPR largely relies on news media and law review articles. A rule that would potentially remake such a large sector of the US economy must rest on the best empirical evidence available, not anecdotes and normative policy arguments.

2. Legal Requirements of a Rule

Under the FTC's organic Magnusson-Moss rulemaking authority, the Commission may proscribe certain conduct that it finds to be either unfair or deceptive. Importantly, this authority is not unlimited. Cognizant of the vast potential scope of the terms "unfair" and "deceptive," Congress only allows the Commission to proscribe acts or practices that are "prevalent," and requires any rule to address specific conduct. These twin conditions are consistent with Section 5's overarching balance between notice and remedy: the FTC—through enforcement or rulemaking—lets actors know exactly what conduct it considers unfair or deceptive, and only after the line between permitted and proscribed conduct is clear can it collect a monetary remedy. Importantly, this balance between knowledge of illegality and remedy played a central role in the Supreme Court's recent decision in *AMG Capital Mgm't v. FTC*, which held that the FTC lacked the power to seek monetary remedies in federal court for first-time violations of the FTC Act.[3]

A. Specificity

The FTC Act requires that any rule "define with specificity acts or practices which are unfair or deceptive."[4] It is easy to see why the specificity requirement is needed; in the limit, absent such a restriction, the FTC could use its Magnusson-Moss rulemaking authority to transform any violation of the FTC Act into a rule violation, and thus subject to monetary remedies. Courts have not had many occasions to address the specificity requirement, yet this relatively thin body of relevant cases provides some important limiting principles. First, the Commission cannot require practices that it thinks would improve the marketplace—and then define failure to adhere to these prescribed practices as an unfair or deceptive act—without first identifying precisely which elements of the status quo are unfair or deceptive, and why.[5]

Second, fealty to the FTC Act's careful balance between notice and remedy requires the FTC to identify the specific acts and practices to be proscribed with sufficient detail to avoid

[3] AMG Capital Mgm't v. FTC, 593 U.S. __, 141 S. Ct. 1341 (2021). For example, the Court pointed to the fact that the FTC Act allows the Commission to obtain monetary remedies against a party only if it violates a cease-and-desist order, engages in conduct the Commission has already condemned in a fully litigated administrative action, or if the conduct was such that a "reasonable man" would have known that it was "dishonest or fraudulent." *Id.* at 1348–49.

[4] 15 U.S.C. 2 § 57a(a)(1)(B). The statement of basis and purposes accompanying any rule must also include "a statement as to the manner and context in which such acts or practices are unfair or deceptive." *Id.* § 57a(d)(1)(B).

[5] *See* Katharine Gibbs School v. FTC, 612 F.2d 658, 661-62 (2d Cir. 1979) (striking down the Vocational School Rule because the FTC failed to "define with specificity" the extant conduct that was "unfair or deceptive," and instead "content[ed] itself with treating violations of [the] 'requirements prescribed for the purpose of preventing' unfair practices [themselves as] unfair practices."); *id.* at 662 ("Requirements designed to prevent unfair practices are predicated upon the existence of unfair practices."); *see also* American Financial Services v. FTC, 767 F. 2d 957, 984 (D.C. Cir. 1985) (distinguishing the Vocational Schools Rule at issue in *Katharine Gibbs* from the Credit Practices Rule, finding that unlike the former, which prescribed requirements designed to prevent "unspecified unfair enrollment advertising and sales practices," the Credit Practices Rule "identifies specific practices . . . as *per se* unfair."). For a full discussion of this issue *see* James C. Cooper*, Privacy Rulemaking at the FTC*, in RULEMAKING AUTHORITY OF THE FTC, (Daniel A. Crane ed. 2022).

offending due process requirements.[6] "Specificity" thus requires a rule to state with "clarity and precision" exactly what conduct it is prohibiting and to describe with "reasonable definiteness" the types of acts or practices that violate the law.[7] In this manner, the specificity requirement would appear to preclude the Commission from issuing a rule that condemned a broad swath of general conduct (e.g., tailored advertising), or that relied on concepts of reasonableness or subjective notions of consumer injury to trigger enforcement.[8]

B. Prevalence

While specificity is a necessary condition for an FTC rule, it is not sufficient. Any rule—even if sufficiently specific in scope—may proscribe an act or practice only when the Commission "has reason to believe" that the conduct covered by the rulemaking is "prevalent."[9] The FTC has only two pathways to satisfy the prevalence requirement: (1) it has issued cease and desist orders regarding such acts or practices; or (2) based on information that "indicates a widespread pattern of unfair or deceptive acts or practices."[10]

If the FTC were to rely on past enforcement to show prevalence, its options for a rule are limited. 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.[11] The sheer number of cases likely allows the FTC to claim that deception about privacy practices is "prevalent," but a broad rule defining material misrepresentations about privacy practices as a deceptive practice likely would fail the specificity requirement, as explained above. The remedy for cases that rest on a deception theory, moreover, is to correct the false representations, not to stop the underlying data practices. Accordingly, a prophylactic rule that banned or required certain data practices, as opposed to an enhanced notice and choice requirement, would be a legally

---

[6] Noting the essential equivalence between an FTC rule and a cease and desist order (whether obtained through administrative or federal court litigation), the Eleventh Circuit has explained that specificity in both FTC rules and orders "is crucial" to avoid due process violations in light of the severity of the penalties a district court may impose. *LabMD v. FTC,* 894 F.3d 1221, 1235 (11th Cir. 2018). The court explained the essential similarities between an FTC rule and an order: "In the litigation context, once an act or practice is adjudged to be unfair, the act or practice becomes in effect—like an FTC-promulgated rule—an addendum to Section 5(a)." *Id.* at 1232.

[7] *Id.* at 1232, 1235; *see also* FTC v. Colgate-Palmolive, Co., 380 U.S. 374, 392 (1965) ("an order's provisions should be clear and precise in order that they may be understood by those against whom they are directed."). This connection with the complaint finds support in the only judicial review of the FTC's use of what has come to be known as its "penalty offense" authority. In addition to being able to seek civil penalties against firms who are parties to an order, the FTC Act also allows the Commission to seek civil penalties from any firm that engages in conduct that the FTC has found to be "unfair or deceptive" in a fully litigated administrative action, but only if the defendant had "actual knowledge" that its conduct violated the FTC Act. 45 U.S.C. § 45(m)(1)(B). In the only case to examine this seldom-used FTC authority, U.S. v. Hopkins Dodge, Inc., 849 F.2d 311 (8th Cir. 1988), the Eighth Circuit held that sending defendants copies and synopses of final orders the FTC had issued against firms involving different industries (e.g., retail meat, beauty products, and real estate) and different practices (e.g., "bait and switch") provided insufficient notice to the defendants to satisfy the "actual knowledge" requirement of section 45(m)(1)(B).

[8] *See LabMD v. FTC,* 894 F.3d 1221 (11th Cir. 2018) (holding that an FTC administrative order that required "reasonable" data security was unenforceably vague).

[9] 15 U.S.C. § 57a(b)(3).

[10] *Id.* at § 57a(b)(3)(A)–(B).

[11] *See* Fed. Trade Comm'n, Federal Trade Commission 2020 Privacy and Data Security Update at 3-5 (May 2021).

problematic cure.[12] It is also worth noting that the element of materiality—while presumed in FTC enforcement actions for deception[13]—may prove a more difficult showing in a rulemaking process given the widespread acknowledgment that consumers rarely read privacy policies, and the role that privacy plays in consumers' actual marketplace choices is uncertain at best.[14]

A rule based on acts and practices alleged to be unfair in past Commission actions would allow the FTC to proscribe certain conduct, but its coverage would be confined to a very limited number of fact patterns. The FTC's Unfairness Policy Statement explicitly states that substantial consumer injury is unlikely to be satisfied by emotional or other subjective harms.[15] To surmount this stricture when charging companies for engaging in an unfair act or practice, the FTC has leaned on potential physical and financial harms that can accompany surreptitious surveillance or unwanted publication of private data. Accordingly, if the FTC relies on past cases to satisfy the prevalence requirement to issue a rule that would ban certain commercial uses of consumer information, it will be limited to a relatively narrow set of data collection practices involving the non-consensual use of precise types of data (e.g., video feeds, real-time geolocation, payment accounts, or sensitive health information)[16] and contexts that increase the likelihood of physical,

[12] For an example of disclosures designed to remedy potentially misleading data practices *see, e.g.*, FED. TRADE COMM'N, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING (Mar. 2013), https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf. The ability of the FTC to mandate disclosure of data practices is also severely limited. Silence about a latent feature of a product is deceptive only when it so fundamentally alters the product beyond consumer expectations as to make it unfit for its intended use. *See* In re International Harvester Co., 104 F.T.C. 949, 1058–59 (1984); Statement of Acting Chairwoman Maureen K. Ohlhausen In the Matter of Lenovo, Inc. (Sept. 5, 2017), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-acting-chairman-maureen-k-ohlhausen-matter-lenovo-inc. Of note, although the FTC has alleged that certain express or implied representations involving data collection and use gave rise to false impressions that required additional disclosure to make them truthful, the FTC has never pursued a "pure" deceptive omission theory in a privacy case. Indeed, it is widely recognized that the FTC Act places no obligation on a firm to provide a privacy policy. *See* Dissenting Statement of Commissioner Maureen K. Olhausen In the Matter of Nomi Technologies, Inc. (Aug. 28, 2015); Dissenting Statement of Commissioner Joshua D. Wright In the Matter of Nomi Technologies, Inc. (Apr. 23, 2015). Although in practice, given mandated disclosure requirements stemming from General Data Protection Regulation (GDPR) and state regimes such as the California Consumer Privacy Act (CCPA), this option may be limited.

[13] *See* 1983 FTC Policy Statement on Deception at 5.

[14] Importantly, whether empirical indifference to privacy is rational or driven by asymmetric information or biases is irrelevant to materiality determinations. The inquiry into materiality is whether consumers would have acted differently but-for the allegedly deceptive representation.

[15] 1980 FTC Policy Statement on Unfairness ("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.").

[16] *See*, *e.g.*, Compl., F.T.C. v. Kochava, Inc., No. 2:22-cv-377 (D. Id. 2022); Compl., United States v. OpenX Technologies, Inc., No. 2:21-cv-09693 (W.D. Cal. 2021); FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. 2017); Compl., In the Matter of PaymentsMD, LLC, No. C-4505 (Feb. 6, 2015).

financial, or reputational harm.[17] Notably, none of these cases have involved the collection or use of consumer information in a routine commercial setting absent some form of deception.[18]

If the FTC were to attempt to pursue the second path and ground its "prevalence" finding on "other information," it must build a record showing a pattern of widespread consumer harm from commonplace online practices. While certain commercial data practices may give rise to privacy concerns, basing a finding of prevalence on information gathered during the rulemaking process itself would require the FTC to override the assumption that consumer behavior generally reflects recognition of one's own self-interest, as well as the available empirical evidence, which, as discussed in more detail below, simply does not support an inference of widespread harm. Rather, it suggests that by-and-large, the data practices that the Commission addresses in the ANPR provide widespread benefits, and that consumers appear willing to provide information to enjoy free online content and services.

3. Costs and Benefits of the Commercial Use of Consumer Information

Consumers value control over their personal information, but they also value many other things and thus must make tradeoffs at the margin based on their opportunity costs and budget constraints. The available empirical evidence suggests that consumers are willing to pay only small amounts to avoid the type of information collection and use in the typical online context, for example those associated with customization of content and ads. Thus, if the Commission ignores the evidence on revealed preferences when developing privacy policy, it is likely to impose large costs on consumers, especially considering the well-documented value that online content providers create from the collection and use of data.

A. Consumer Value of Privacy and Personal Information Flows[19]

In what has come to be known as the "privacy paradox," stated preferences (e.g., surveys and polls) tend to show that consumers care deeply about privacy, but revealed preference—data from actual choices—suggests that they are willing to share personal information for relatively

[17] For example, the FTC has used unfairness to address non-consensual surveillance of intimate activity. *See* In re Support King, LLC, No. C-4756 (F.T.C. Dec. 20, 2021); In re Zoom Video Communications, Inc., No. C-4731 (F.T.C. Jan. 19, 2021); In re Retina-X Studios, LLC, No. 172-3118, 2020 WL 1549673 (F.T.C. Mar. 26, 2020); In re TRENDnet, Inc., No. C-4426 (F.T.C. Feb. 7, 2014); In re DesignerWare, LLC, No. C-4390 (F.T.C. Apr. 15, 2013). The FTC has also used unfairness to address non-consensual collection and use of data that may lead to reputational or other financial harms. *See*, *e.g.*, Compl., United States v. Mortgage Solutions FCS, Inc., No. 4:20-cv-00110 (N.D. Cal. Jan. 7, 2020); In re Facebook, Inc. No. C-4365, 2012 WL 3518628 (F.T.C. July 27, 2012).

[18] *See*, *e.g.*, Dissenting Statement of Commissioner Noah Phillips, 87 Fed. Reg. 51273, 51295 ("We have never brought a case alleging that targeted advertising is unfair. The Commission has brought cases where companies deceptively collected, used, or shared personal data for purposes including targeting advertising, that that is not the same.").

[19] It is important to distinguish between intrinsic and strategic (or instrumental) demand for concealing certain information in certain contexts. While *ceteris paribus* increased provision of the former provides increased utility to consumers, strategic privacy—concealment of private information to secure advantage in commercial or social transactions—is often welfare-reducing, as it introduces asymmetric information problems and exacerbates adverse selection and moral hazard. *See* Tesary Lin, *Valuing Intrinsic and Instrumental Preferences for Privacy*, 41 MARKETING SCI. 663, 673-76 (2022) (measuring consumers' intrinsic and instrumental values of revealing certain types of information in a commercial context); James C. Cooper, *Separation Anxiety*, 21 VA. J.L. TECH. 1 (2017).

low prices.[20] For example, a recent Pew Research Center poll finds that 81 percent of Americans say that the privacy risks associated with companies' data collection outweigh the benefits.[21] At the same time, 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 in the typical online context.[22] Prince and Wallsten, for instance, use a discrete choice experiment and find that, on average, US consumers are only willing to pay a monthly fee of $1.82 to avoid location tracking and $3.75 for browsing across different platforms.[23] Employing a similar methodology, Savage & Waldman find that consumers are willing to pay a one-time fee of $2.28 for an app that does not track browsing and $1.19 for an app that does not track location.[24] In another experiment, Strahilevitz and Kugler find that Gmail users who are educated about Google's privacy policy regarding the use of email content to target ads believe the practice is invasive, but nonetheless agree that they have consented to this privacy invasion in return for free email.[25] Further, only 35 percent of these users would be willing to pay any amount for a version of Gmail that did not use email content analysis to serve ads, and of this minority, the median willingness to pay was $15.[26] Consistent with these findings, a recent field experiment shows that sophisticated undergraduate students were willing to trade personal information when presented with small costs to protect (or small incentives to reveal) this information, a result that held regardless of a student's stated privacy preferences.[27] Multiple studies have found similar results.[28]

---

[20] *See, e.g.*, CMA Report, *Appendix F*, at ¶ 4.47 ("[I]n surveys, consumers will report that they are very concerned about their privacy but they then behave in a way that contradicts this clearly stated preference by, e.g., not taking advantage of privacy controls that are available to them."); Acquisti, Taylor, & Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442, 476-478 (2016).

[21] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused, and Feeling a Lack of Control over Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[22] *See* Aquisti, Taylor, and Wagman, *supra* note 20, at 479.

[23] 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).

[24] Scott J. Savage & Donald M. Waldman, *Privacy Tradeoffs in Smartphone Applications*, 137 ECONOMIC LETTERS 171, 173-74 (2015).

[25] *See*, *e.g.*, Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. LEGAL STUD. S69, S77-80 (2016)

[26] *Id.*

[27] Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, NBER Working Paper at 8-14 (Sept. 27, 2017).

[28] *See* Tesary Lin, *supra* note 19, at 674 (in an experimental setting, estimated that on average consumers would be willing to accept $10.34 to reveal income, gender, age, education, relationship status, information about children, zipcode, and race); Michael Kummer & Patrick Schulte, *When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications*, 65 MGMT. SCI. 3470, 3477 (2019) (finding implied estimates that consumers are willing to pay .02-.03 Euros to avoid apps with sensitive permissions, and suppliers willing to reduce their prices by .24 Euros for an app with sensitive permissions); Alessandro Acquisti et al, *What is Privacy Worth?*, 42 J. LEG. STUD. 249, 267 (2013) (finding evidence that consumers placed a higher value on privacy when endowed with a privacy-enhancing payment card, and that overwhelming majority of consumers willing to accept $2 to have their gift card purchases tracked); Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254, 264-65 (2011) (in an experimental setting finding that consumers were willing to pay approximately $0.60 more to purchase batteries and sex toys from merchants with better and more salient privacy policies); *also* Jane Bambauer et al., *A Bad Education,* 2017 IL. L. REV. 109 (2017); Adam S. Chilton & Omri Ben-Shahar, *Simplification of Privacy Disclosures: An Experimental Test,* 45 J. LEG. STUD.

In harmony with these empirical studies, we do not observe consumers taking readily available and cheap options to limit firms' ability to track them online. For example, empirical research finds that only a tiny percentage of consumers actually choose to opt out of online tracking.[29] Further, in the leading survey of the economics of privacy, the authors conclude, "If anything, the adoption of privacy-enhancing technologies (for instance, Tor, an application for browsing the Internet anonymously) lags vastly behind the adoption of sharing technologies (for instance, online social networks such as Facebook)."[30] Additionally, there is little evidence to suggest that highly visible attempts to compete on privacy have had much impact on consumer behavior.[31]

Because the online data ecosystem is complex, there are reasons to believe that consumers may lack perfect knowledge regarding the collection and use of personal information. Nonetheless, there is no reason the Commission should ignore revealed preferences—whether measured in the lab or in the field—involving information-sharing tradeoffs in the context of typical online interactions.[32] Surely these shed some insight into hard-to-observe actual consumer

---

41 (2016); Alessandro Acquisti, *Privacy and Human Behavior in the Age of Information,* 347 SCIENCE 509 (2015) (providing a summary of related scholarship); Jan H. Schumann et al., *Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance Among Users of Free Web Services,* 78 J. MARKETING 59 (2014); Kai-Lung Hui et al., *The Value of Privacy Assurance: An Exploratory Field Experiment,* 31 MIS QUARTERLY 19 (2007); Eric J. Johnson et all., *Defaults, Framing and Privacy: Why Opting In-Opting Out,* 13 MARKETING LETTERS 5 (2002).

[29] *See* Garrett A. Johnson, Scott K. Shriver, & Shaoyin Du, *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?,* 39 MARKETING SCI. 33, 40 (2020) (finding that 0.23 percent of display advertising impressions are served to consumers who have opted out of online tracking through the AdChoices program).

[30] Acquisti, Taylor, & Wagman, *supra* note 20, at 476.

[31] For example, DuckDuckGo increased its advertising spending by over 80% in recent years, yet its market share has continued to hover around 2.5 percent. *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/; *also* Search Engine Market Share United States Of America, statcounter (accessed on Oct. 16, 2022), https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america. See also *See also* Danny Sullivan, *Is Microsoft's Scroogled Campaign Working? Not if Gaining Consumers is the Goal*, MARKETING LAND (Oct. 16, 2013), https://marketingland.com/microsoft-scroogled-campaign-61887/.

[32] Some privacy scholars have suggested that the privacy paradox is illusory, primarily because survey instruments tend to ask broad questions about privacy as an overall value, while actual privacy choices are highly contextual. For example, Martin & Nissenbaum argue that there is nothing inconsistent with placing a high value on privacy and sharing information if one's expectations about how the data are used are met. They provide the results of several vignette studies that show how consumers' views on whether their privacy expectations are met vary among several dimensions. *See*, *e.g.*, Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables*, 18 COLUM. SCI. & TECH. L. REV. 177 (2016). In a similar vein, Solove suggests that empirical studies on consumer choices "reveal[] preferences in specific situations." Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 24 (2021). We make no claim that the revealed preference studies provide evidence that consumers do not value privacy. Rather, these studies provide empirical evidence that when faced with a trade-off in the specific context of personal information flows related to commonplace online commercial uses, consumers do not demand large payments to permit such flows. Absent deception, embedded in these decisions are the risks associated with uses that are incompatible with expectations and thus may be harmful. For this reason, these revealed preference studies are highly relevant to the Commission's Commercial Surveillance ANPR. Solove also claims that revealed preference studies can tell us nothing about consumer valuation of privacy because they concern "risk," which "involves the potential for harm," while "value" is "overall importance." *Id*. at 24. In many ways, this

preferences. Theories that dismiss the importance of revealed preferences (e.g., by hypothesizing that consumers are "resigned" to giving away data to companies)[33] do not and cannot rule out the more parsimonious explanation that their concerns about privacy are adjusted up or down depending on the perceived costs and benefits of each specific data practice and transaction. Context-specific privacy concerns about a data practice can be outweighed by the context-specific benefits.[34] After all, some experiments have expressly educated consumers on the privacy intrusiveness of their choices and found little or no impact on consumer behavior.[35] Further, empirical research has demonstrated that free online social networks and search engines generate tremendous amounts of consumer surplus.[36] Thus, consumers could place a high value on the information they share, but place an even higher value on the services they receive.

What is more, consumer understanding of how online content providers collect and use data is endogenous: the marginal cost of gathering and processing information, combined with the marginal benefits from having greater information surrounding the particular decision at hand determines the level of information asymmetry consumers accept. Thus, consumers rationally incur the costs of gathering and processing additional information to make decisions when they perceive that being wrong is even *more* costly. That consumers make decisions surrounding the collection and use of personal information with imperfect knowledge of risks and benefits might simply reflect that they have a low expected harm from online tracking. Finally, it is important to note that firms have incentives to make privacy practices that are superior to their competitors

---

is merely a semantic issue; as noted, we make no claim that revealed preference studies provide evidence of consumer valuation of privacy in *all* circumstances or that they are answering the same questions as broad privacy survey questions. Nonetheless, the choice to take payment to accept a risk (or to purchase insurance to avoid a risk), provides information on the underlying value (willingness-to-pay or willingness-to-accept) of what is at risk. Thus, experiments or field studies that provide estimates of willingness-to-pay to avoid some type of information collection or use (or willingness to accept to share information) capture risk calculations, risk preferences, and the value one places on possible harmful uses of the data. For example, holding the probability of destruction and risk preferences constant, a consumer will be willing to pay more to insure a $1 million home than a $100k home.

[33] *See*, *e.g.*, ANPR at 51,274 ("Reports suggest that consumer have becomes resigned to the ways in which companies collect and monetize their information, largely because consumers have little to no actual control over what happens to their information once companies collect it.").

[34] Long Chen et al., *The Data Privacy Paradox and Digital Demand,* NBER WORKING PAPER NO. 28854, AT 21-25 (2021) (finding that individuals who have the greatest concern for privacy also get the greatest value from data-sharing); Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms,* 30 BUS. ETHICS QUART. 65, 72 (2019) (summarizing this literature) ("Uses of information deemed privacy violations in consumer surveys may be better judged after taking into consideration the benefits of sharing information online."); Susanne Barth & Mennode Jong, *The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review,* 34 TELEMATICS AND INFORMATICS 1038, 1044-50 (2017); *generally* Heng Xu et al., *The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services,* 26 J. MGMT. INFO. SYS. 135 (2009); Hui et al., *supra* note 28; Tamara Dinev & Paul Hart, *An Extended Privacy Calculus Model for E-Commerce Transactions,* 17 INFO. SYS. RESEARCH 61 (2006); Culnan & Bies, *Consumer Privacy: Balancing Economic and Justice Considerations*, 59 J. Social Issues 2 (2003).

[35] *See*, *e.g.*, Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. LEGAL STUD. S69 (2016); Omri Ben-Shahar & Adam S. Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. LEG. STUD. S41 (2016).

[36] *See* Eric Brynjolfsson et al., *Using Massive Online Choice Experiments to Measure Changes in Well-being*, 116 PNAS 7250, 7251-53 (2019).

salient to consumers if credible disclosures are not too costly to make, and they expect consumers to respond favorably to such disclosures.[37]

A complete evaluation of the value of privacy to consumers (or the cost to consumers when data is collected and used in the digital economy) must also consider differing levels of sensitivity to privacy. The risks and harms associated with a data practice are interpreted, at least to some degree, through an individual's experience of loss of dignity, loss of a sense of control, and upset expectations.[38] These will vary not only by data practice but also by person. Some people are much more privacy-sensitive than others,[39] and even individuals who have the same average privacy sensibilities may still have different expectations and dignitary losses depending on who is accessing data or for what purpose.[40] The "messy middle" category includes data practices where some individuals are willing to relinquish control and others are not. For example, some consumers prefer to disclose information for the purpose of content personalization or to access free services while others do not.[41] This means that the benefits of strict privacy controls will be mixed. While privacy-sensitive individuals will prefer having new protections and consent-based control over their information, others who are privacy pragmatists could see data subject control as a cost in some circumstances because it creates an imposition on them to manage requests and opt-ins for services that are, in their mind, clearly worth it.[42] Some individuals might perceive consent procedures as getting in the way of the usefulness of the data. For example, as discussed in more detail below, data practices that are designed to detect fraud would be undermined if the target of an investigation had to be consulted in advance. Also, data practices that depend on a representative sample of data to accomplish their goals could suffer

---

[37] This is the general result of Paul Milgrom, *Good News and Bad News: Representations Theorems and Applications*, 12 BELL J. ECON. 380 (1981). For a review of the conditions under which unraveling is likely to happen and the empirical literature on unraveling *see* David Dranove & Ginger Zhe Jin, *Quality Disclosure and Certification: Theory and Practice*, 48 J. ECON. LIT. 935 (2010); *also* David Butler & Daniel Read, *Unravelling Theory: Strategic (Non-) Disclosure of Online Ratings*, 12 GAMES 73 (2021) (finding evidence of partial unraveling for hotels); Pauline M. Ippolito & Alan D Mathios, *Information, Advertising and Health Choices: A Study of the Cereal Market*, 21 RAND J. ECON. 459 (1990) (finding evidence to support unraveling on fiber content in the breakfast cereal market).

[38] Daniel Solove, *A Taxonomy of Privacy,* 154 U. PENN. L. REV. 477, 507 (2006) (describing the harms from data aggregation. Note that Solove also describes significant economic benefits as well and does not take a position on whether or when privacy harm occurs from aggregation and reuse.).

[39] Alan Westin found that a sizable subset of individuals was privacy-unconcerned, some were pragmatists (willing to trade privacy for benefits), and some were privacy sensitive. Alan F. Westin, *Social and Political Dimensions of Privacy,* 59 J. SOCIAL ISSUES 431, 445 (2003) (describing survey work conducted in the 1990s).

[40] The same person also has different privacy preferences over time. *See* Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns,* 102 AM. ECON. REV. 349 (2012).

[41] Xu et al., *supra* note 34, at 153-58; Syagnik (Sy) Banerjee & Ruby Roy Dholakia, *Mobile Advertising: Does Location Based Advertising Work?,* 3 INT'L. J. MOBILE MARKETING 68 (2008).

[42] Outside Facebook, where sustained attention and criticism have caused a greater proportion of users to change their privacy settings (Andrew Perrin, *Americans Are Changing Their Relationship with Facebook,* PEW RESEARCH CENTER (2018), available at http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/), the great majority of consumers do not bother to change default settings related to their privacy. This is true even in Europe, where only 12.5% of Europeans opt out of data collection despite the very prominent and easy-to-use pop-up windows providing the opportunity to do so. Guy Aridor et al., *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR,* NBER WORKING PAPER NO. 26900 (2021).

from selection bias if only some potential data subjects opt in.[43] Thus, tools meant to address privacy can exacerbate the algorithmic bias problems that are also referenced in the ANPR.[44]

To be clear, we are not arguing that the available evidence shows little or no consumer value in privacy. On the contrary, much of the empirical evidence can be consistent with the popular idea that when we use free online services, we "pay with our privacy." But the fact that consumers would prefer to not "pay" does not alone prove that data collection and use practices are harmful. After all, consumers would also prefer to not pay using money, all things being equal. Our point, rather, is that "paying with data" may very well be cheaper to most consumers than the price that service providers would charge in the absence of a data trade. Thus, prohibitions on a business model that allows people to pay with data will remove a form of trade that has a better value for most consumers.

B. Value to Consumers and Firms from the Collection and Use of Information

The available empirical evidence also provides strong evidence that the type of personalization made possible by the collection and use of consumer information provides both consumers and firms with substantial benefits. More specifically, personalization improves the match between users and content or services, for example through better matching to advertisers, curated content, better matching to other users, better matching to tools or functionality within an application, and better protection against fraud and other harmful behavior.

Tailored Advertising. The consensus in the empirical literature is that advertisements based on cookies and other identifiers provide approximately two- to three-times more revenue on average than those based on context alone.[45] This premium reflects higher conversion rates—that is, there is a higher probability that a voluntary value-enhancing exchange will occur in response to advertising served on consumer interests rather than on context alone. Several empirical papers have used the GDPR to estimate the causal impact of a reduced ability to track customers—and the concomitantly reduced capability to tailor ads— on economic outcomes for firms. For example, Goldberg et al., estimated lower-bound reductions in real (as opposed to

---

[43] Jane Yakowitz Bambauer, *Tragedy of the Data Commons,* 25 HARV. J. L. & TECH. 1, 61, 64 (2011) (published as Jane Yakowitz).

[44] *See* ANPR at 51283-84.

[45] *See*, *e.g.*, CMA Report on the Digital Economy, Appendix F, at F31-32, F36 (2020) (70% lower without identifier); Garrett A. Johnson et al., *Consumer Privacy Choice in Online Advertising: Who Opts Out and at what Cost to Industry?*, 36 MARKETING SCI. 33 (2020) (52% lower without identifier); Rene Laub et al., *The Economic Value of User Tracking for Publishers* (2022) (24% lower without identifier), *at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4251233; Ravichandran & Korula, *The Effect of Disabling Third-party Cookies on Publisher Revenue*, Google Tech. Rep. (2019) (52% lower without identifier); Howard J. Beales & Jeffrey A. Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, Navigant Economics (2014) (66% lower without an identifier); Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising*, 57 MGM'T SCI. 57 (2011) (65% lower without identifier). *But see* Veronica Marotta, Vibhanshu Abhishek, & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis* at 6-7, 14-16, 27 (2019) (finding a statistically insignificant 4% reduction in the value of an impression without an identifier), *at* https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

recorded) pageviews and online purchasing, of 7 percent and 4.6 percent, respectively.[46] Likewise, Aridor et al. examine the impact of the GDPR on online travel websites and search engines and find a statistically and economically significant reduction in advertising clicks and a short-term reduction in advertising revenues.[47] Focusing on the effects of GDPR on investment decisions, Jia et al., find that the GDPR, by increasing compliance costs and reducing the expected revenue streams from consumer data, significantly reduced venture capital investment in EU technology startups—a result that appears to be persistent.[48]

Services and Content. Because tailored advertising generates more revenue for content providers than contextual advertising, it can help provide more, and higher quality online content and services.[49] What is more, to the extent that personalization features described above increase the number of users, and thus available advertising inventory, it also generates more revenue for the content provider, further amplifying the ability to provide more and better-quality content. The ability to collect consumer information also allows online firms to perform analytics to improve their content.[50]

Several empirical studies have found an inverse relationship between content and restraints on data collection and use. Shiller et al., for example, find a causal relationship between the intensity of users employing ad-blocking technology and various metrics of website quality.[51] Similarly, preliminary research from Janssen *et al*. finds that GDPR's restrictions on data collection and use have increased exit and reduced entry of Android apps, and they estimate that this loss in content has reduced consumer surplus by 32 percent.[52] Also suggesting a

---

[46] *See* Goldberg et al., *Regulating Privacy Online: An Economic Evaluation of the GDPR*, at 3, 33 (May 31, 2022).

[47] Guy Aridor, Yeon-Koo Che, & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from the GDPR*, NBER Working Paper at 24-27 (forthcoming RAND J. ECON, 2022). The reduction in advertising revenue falls by (as statistically significant) 25 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. As the authors note, this is likely due to a gradual 12% increase in the average bid, likely due to the fact that post-GDPR observable consumers have more observable conversion rates. *Id.*; s*ee also* Christian Peukert et al., *Regulatory Spillovers and Data Governance: Evidence From the GDPR*, 41 MARKETING SCI. 746, 754-61 (2022) (finding substantial reductions in interactions with third-party data vendors after GDPR).

[48] *See* Jia et al., *The Short-Run Effects of GDPR on Technology Venture Investment*, 40 MARKETING SCI. 661, 667-80 (2021); Jian Jia, et al., *The Persisting Effects of the EU General Data Protection Regulation on Technology Venture Investment*, THE ANTITRUST SOURCE (Jun. 2021).

[49] Because demand for content is inversely related to price, the first-order effect of a reduction in output is a reduction in consumer welfare. The value to consumers of the lost content is uncertain. It could be that lost content is the lowest valued content (because it was on the margin). Alternatively, quality might be stochastic *ex ante*, so that some of the content we do not see might have been quite valuable to consumers.

[50] *See*, *e.g.*, CMA Report on Digital Economy, Appendix F, at ¶ 129-131 (discussing the importance of the use of data in verification and attribution); Nils Wernerfelt et al., *Estimating the Value of Offsite Data to Advertisers on Meta* (2022) (finding cost of incremental customer acquisition rises, especially for small businesses, without access to third-party conversion data), *at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176208.

[51] Benjamin Shiller et al., *The Effect of Ad Blocking on Website Traffic & Quality*, 49 RAND J. Econ. 43, 51-58 (2018); *see also* Garrett Johnson, Tesary Lin, & James C. Cooper, COPPAcalypse? *The YouTube Settlement's Impact on Kids Content*, University of Pennsylvania, Economics of Digital Services Working Paper 4, 7, 13-14 (Sept. 1, 2022) (finding that the elimination of cookies for made-for-kids (MFK) content on YouTube resulted in a reduction of new video uploads for MFK channels), available at https://www.law.upenn.edu/live/files/12330-coppacalypse-the-youtube-settlements-impact-on.

[52] Rebecca Janssen et al*., GDPR and the Lost Generation of Innovative Apps*, NBER Working Paper at 2, 14 (May 2022).

positive relationship between data use and content quality, recent research finds that users' ratings of Google Play Store apps are inversely related to their privacy grades.[53] Other works examining the effect of the GDPR on content have found more mixed results. For example, Lefrere et al. find a small decrease in page views for EU news and media publishers relative to their US counterparts after the GDPR, but they find no statistically measurable impact in other dimensions, such as social media engagement with content or page rank, and suggest that these null results might reflect firms' continuing access to consumer data through GDPR exceptions.[54]

Big data applications outside social media and websites also exhibit a positive relationship between data use and quality. In the health sector, for example, advances in Machine Learning are changing the practice of medicine because new programs can digest and learn from vast amounts of data about both the patient and others to make customized, time-sensitive recommendations.[55] Data-driven medical adherence scoring systems, which use information about patients to predict whether they are likely to stick with a prescribed treatment, can improve health by better matching patients to services, such as treatments and pharmacy interventions.[56]

Avoiding Fraud and Malfeasance. Finding reliable information about business partners, clients, and customers is a specific example of a market transaction cost. Just as consumers often need information about businesses in order to have confidence that they will not be defrauded, deceived, or mistaken about the quality of goods and services, businesses, too, sometimes need information about their clients and customers to avoid losses from fraud or to protect the safety or wellbeing of other customers. These companies will naturally want to reduce risks by using information about the reliability of users and consumers who do not yet have a track record with the firm.[57] If the risks can't be avoided, the firm will have to increase prices or decrease quality to compensate for the firm's losses.

The available empirical evidence bears this out. For example, credit markets provide ample evidence that credit becomes more available, and at lower interest rates, when banks can use more personal information to better assess the risk of credit default. In the absence of credit scores and other personal data details, banks would be forced to treat loan applicants in crude categories, based on applicant income or the value of the collateral, instead of making more fine-

---

[53] James C. Cooper & John M. Yun, *Privacy & Antitrust: It's Complicated*, 2022 ILL. J.L. TECH & POL'Y 382, 393 (2022). This finding could be due to developers that lack data (and thus have a higher privacy grade) being unable to improve or personalize the experience in the app or due to reduced revenues from an inability to personalize advertising, resulting in less investment in the quality of the app.

[54] V. Lefrere et al., *Does Privacy Regulation Harm Content Providers? A Longitudinal Analysis of the Impact of the GDPR,* at 7, 48 (2022), *at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4239013; *see also* Miguel Godinho de Matos & Idris Adjerid, *Consumer Consent and Firm Targeting After GDPR: The Case of a Large Telecom Provider*, 68 MGM'T SCI. 3330 (2022) (finding that opt-in for different data types increased after GDPR-compliant consent forms were re-solicited, resulting in increased sales to those who were treated with the GDPR-compliant consent).

[55] *See*, *e.g.*, the discussion of Ginger.io in Basel Kayyali et al., *The Big-Data Revolution in US Health Care: Accelerating Value and Innovation,* MCKINSEY REPORT (2013). Some of the most promising applications would have to merge data from disparate sources both within and outside the health sector, and the incentives to do this are likely to depend on being able to collect, purchase, and reuse personal data. Sonja Marjanovic et al., *Understanding Value in Health Data Ecosystems,* RAND RESEARCH REPORT (2017).

[56] *See* Inmaculada Hernandez & Yuting Zhang, *Using Predictive Analytics and Big Data to Optimize Pharmaceutical Outcomes,* 74 AM. J. HEALTH-SYST PHARM. 1494 (2017).

[57] Richard A. Posner, *The Right to Privacy,* 12 GA. L. REV. 393, 394-95 (1978).

grained lending decisions based on the applicant's history of reliability. Thus, independent sources of information that can reassure lenders about the creditworthiness of a loan applicant help the *applicant* as much as they help the lender.[58] While there may be some threshold beyond which additional data is not useful for improving matching and performance, society has not reached that threshold. A study of home loans in the San Francisco Bay area found that loan applicants living in the counties that prohibited banks from using financial data without an applicant's opt-in consent paid higher interest rates and defaulted more often than similar loan applicants living in counties that had more permissive privacy rules because banks could not match applicants to loans as well.[59]

***

That personalization leads to well-documented consumer benefits, coupled with observed consumer behavior, appears to contradict the core proposition underlying the ANPR—namely, that restrictions on the collection and use of data employed to make such personalization possible are needed to prevent "prevalent" and "widespread" consumer harm. On the contrary, the empirical evidence strongly suggests that the FTC's current case-by-case approach that targets specific unfair or deceptive practices that may harm consumers in the online commercial context is far more appropriate than a broad rule.

4. Privacy and Competition

As a threshold matter, we note that the FTC is unlikely to possess the authority to issue rules under its power to proscribe "unfair methods of competition."[60] The only court to address the issue did so fifty years ago, and it is doubtful that its rationale would survive today, especially when one looks at the obscure provision purported to give the FTC such broad power (section 6(g))[61] in the context of the entire structure of the FTC Act.[62] Second, there are unlikely to be any privacy-threatening data practices that would fit into the small compartment of behavior that current antitrust laws condemn per se, yet this is precisely what an unfair methods of competition (UMC) rule would do. Not only would this misalignment between a UMC rule targeting data practices and modern antitrust precedent signal bad policy, but it also suggests that the FTC would have trouble defending such a rule as a "reasonable interpretation" of its organic statute under any *Chevron* analysis.[63]

---

[58] *See* Cooper, *Separation Anxiety*, *supra* note 19, at 25-31(providing a summary of empirical literature on the advantages of credit scoring to underserved communities).

[59] Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis,* 46 RAND J. OF ECON. 1, 13-18 (2015). This is consistent with the more general phenomenon of risk-based lending markets. *See also* Wendy Edelberg, *Risk-Based Pricing of Interest Rates for Consumer Loans,* 53 J. MONETARY ECON. 2283 (2006).

[60] For a full discussion of this issue *see* James C. Cooper*,* Privacy Rulemaking at the FTC, in RULEMAKING AUTHORITY OF THE FTC (Daniel A. Crane ed. 2022).

[61] 15 U.S.C. § 46(g).

[62] National Petroleum Refiners Association v. FTC, 482 F.2d 672 (D.C. Cir. 1973).

[63] Chevron U.S.A., Inc. v. NRDC, 467 U.S. 837 (1984).

Leaving aside issues surrounding the FTC's legal authority to promulgate UMC rules, as a policy matter, there is little reason to believe that there is a link between the routine collection and use of consumer data and the accretion and use of market or monopoly power.[64] First, as discussed above, consumers do not appear to alter their consumption choices based on privacy concerns to a degree that would suggest that privacy is an important dimension of competition. If consumers do not respond to firms' privacy choices, privacy cannot be an important dimension of competition, which undermines any link between market power and lower levels of consumer privacy.[65]

A second factor undermining the link between market power and the commercial collection and use of consumer data is that data is an input into a larger production process that creates consumer value through greater customization and more relevant content, as discussed above.[66] Because privacy costs and data benefits work in opposite directions, and because the demand for privacy and a platform's product are heterogenous and potentially correlated in complicated ways, the relationship between increased data collection and consumer welfare is ambiguous.[67] Recent empirical work is consistent with these theoretical results, suggesting no link between market power and reduced levels of privacy.[68]

Although regulation of the use of online identifiers is unlikely to have any positive impact on competition, the converse is not true. For example, consent-based privacy controls can work at odds with competition policy goals because the companies that are in the best position to collect and manage consents and to combine a larger variety of types of data are often

---

[64] For a full discussion of the link between privacy and competition *see* James C. Cooper & John M. Yun, *Privacy & Antitrust: It's Complicated*, *supra* note 53.

[65] Alex Marthews & Catherine Tucker, *Privacy Policy and Competition*, ECON. STUD. BROOKINGS at 8 (Dec. 2019) ("There is little evidence that competition itself appears to enhance privacy.")

[66] For example, when two competing firms merge and, *ceteris paribus*, raise their combined price as a result, consumers are unambiguously worse off. The same cannot be said if two competing firms increase the collection and use of consumer data after a merger, because these data have value only when they are monetized—and as discussed above, monetization creates benefits for consumers. Even monetization of data that generates no direct benefit to consumers (such as selling to a data broker) will generate marginal revenue streams that are likely to be passed along to users (directly in the form of lower prices or indirectly in the form of enhanced content). In this context, we can model increased revenue streams from selling consumer data as a reduction in a firm's marginal cost. *See* Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. TELECOM & HIGH TECH L. 251 (2012).

[67] *See, e.g.*, Michael L. Katz, *Multisided Platforms, Big Data, and a Little Antitrust Policy*, 54 Rev. Indus. Org. 695, 707 (2019) ("[I]t is not evident that competition promotes privacy or, indeed, that promoting greater levels of privacy is desirable. There is no general theorem that states that competitive firms offer higher-quality products than monopolists or that monopolists undersupply quality. Similarly, there is no general result stating that a firm with market power undersupplies privacy or that an increase in competition will lead to an increase in privacy."). If some consumers find reductions in privacy accompanied by concomitant product quality increases on net beneficial, changes in privacy lead to shifts and rotations in demand. The direction and size of the rotation (clockwise or counterclockwise), and hence the net impact on welfare, depends on the correlation of the distributions of preferences for privacy and quality improvements. *See* Daniel P. O'Brien & Douglas Smith, *Privacy in Online Markets: A Welfare Analysis of Demand Rotations*, Fed. Trade Comm. Bureau of Economics Working Paper No. 323 (2014), https://www.ftc.gov/system/files/documents/reports/privacy-online-markets-welfare-analysis-demand-rotations/wp323.pdf.

[68] *See* James C. Cooper & John M. Yun, *supra* note 53 (Using a variety of methodologies, the authors find no statistical relationship between objective metrics of Android apps, popular website privacy practices, and various market concentration measures).

the same companies that already dominate their markets.[69] Several studies find that the GDPR is associated with increases in the market shares of large third-party data vendors.[70] Further, private decisions to restrict the flow of consumer information to foster higher privacy standards have met with antitrust scrutiny. For example, Google's restricting the flow of user identification data to third parties was alleged to constitute illegal exclusionary conduct in the recent monopolization case led by the Texas Attorney General.[71] At the same time, Google has faced allegations that *sharing* these data with third parties has violated the GDPR[72] and California privacy laws.[73] Similarly, Google's announced movement away from third-party cookies led to an investigation by the UK's Competition Market Authority for its potential impact on rivals in the ad tech space.[74] The result was a commitment by Google to not proceed without consultation and collaboration with the CMA, and that it would not take actions that would provide itself with an advantage in the digital advertising space.[75]

Finally, compliance costs must not be ignored. Using GDPR as an example, the internal budgets for privacy offices at companies of all sizes (including in the U.S.) increased by 29 percent.[76] Costs to American companies that must comply with GDPR-style laws are estimated to be approximately $480 per data subject.[77] These compliance costs cause the prices that consumers pay to rise—a cost that may well be worth it to some people and in some contexts, but should not be presumed to be worth it for *most* people in *most* contexts.

---

[69] For a theoretical model predicting that privacy regulation will tend to reduce the competitive structure of data-intensive industries, *see* James Campbell et al., *Privacy Regulation and Market Structure,* 24 J. ECON. & MGMT STRATEGY 47 (2015).

[70] *See* Garrett Johnson et al., *Privacy and Market Concentration: Intended & Unintended Consequences of the GDPR* (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686; s*ee also* Christian Peukert et al., *Regulatory Spillovers and Data Governance: Evidence From the GDPR*, 41 MARKETING SCI. 746 (2022); Ran Zhuo et al., *The Impact of the General Data Protection Regulation on Internet Interconnection,* NBER WORKING PAPER NO. 26481 (2020).

[71] In re Google Digital Antitrust Litig., Case No. 21-CV-6841, Compl. at ¶¶ 135-152 (S.D.N.Y); *see* In re Google Digital Advert. Antitrust Litig., 2022 WL 4226932, at *24 (S.D.N.Y. Sept. 13, 2022) ("[T]he Complaint does not plausibly allege that Google's refusal to share unencrypted user IDs amounted to anticompetitive conduct.").

[72] *See* John Koetsier, *Alleged Global Google Privacy Leak: 'GDPR Workaround' Could Incur $5.4B Fine*, FORBES (Sep. 4, 2019), https://www.forbes.com/sites/johnkoetsier/2019/09/04/alleged-global-google-privacy-leak-gdpr-workaround-could-incur-27b-fine/.

[73] *See* Hewitt v. Google LLC, Case 5:21-cv-02155 (N.D. Cal., Mar. 26, 2021).

[74] UK's Competition & Markets Authority, *CMA to Investigate Google's 'Privacy Sandbox' Browser Changes* (Jan. 8, 2021), https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes.

[75] *See* UK'S COMPETITION & MARKETS AUTHORITY, NOTICE OF INTENT TO ACCEPT COMMITMENTS OFFERED BY GOOGLE IN RELATION TO ITS PRIVACY SANDBOX PROPOSALS, Case No. 50972 (June 11, 2021), https://assets.publishing.service.gov.uk/media/60c21e54d3bf7f4bcc0652cd/Notice_of_intention_to_accept_binding_commitments_offered_by_Google_publication.pdf. Not only has private conduct aimed at improving privacy been critiqued as anticompetitive, but consumer privacy has been recognized as a justification for allegedly anticompetitive conduct in antitrust suits. *See* Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J. FORUM 647, 664-68 (2021) (discussing antitrust cases with privacy justifications). The most recent example is Apple relying on consumer privacy and security to explain its allegedly anticompetitive app-store restrictions in *Epic Games v. Apple*. Epic Games v. Apple, Inc., 4:20-cv-05640 (N.D. Cal. 2021).

[76] *IAPP-EY Annual Privacy Governance Report 2021*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP) (2021).

[77] Alan McQuinn & Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (ITIF), at 4-18 (2019).

5. First Amendment

The ANPR does not ask for comments on how a potential privacy rule would be designed to comply with First Amendment restrictions even though all the practices discussed by the ANPR (collecting information, using it to generate new inferences, or using it to curate content and advertising) are forms of protected expression. In *Sorrell v. IMS Health Inc.*, the Supreme Court struck down a state law that prohibited the use of a doctor's prescribing data for targeted advertising purposes without the doctor's consent.[78] That case applied strict scrutiny because the law at issue imposed speaker-based restrictions on the use of personal data to tailor the advertising of only one industry (drug manufacturers).

If the Commission uses rulemaking to restrict or ban all targeted advertising regardless of content or speaker, the rule might trigger only intermediate scrutiny under the *Central Hudson* test for commercial speech.[79] But a broad restriction would fail even the intermediate scrutiny test, which requires that the law further a substantial government interest and the restriction is well-tailored to that interest because it would be hard to justify in light of the paucity of evidence of consumer harm. Indeed, the ban would have such a negative impact on publishers that the consumers are likely to be harmed, indirectly, by a restriction on behavioral advertising rather than helped by it. Even if a court found that an FTC rule restricting targeted advertising serves a substantial government purpose, the rule is likely to fail a tailoring analysis unless the Commission takes care to avoid dampening advertising more than necessary to serve privacy-sensitive consumers' interests (e.g., an opt-out system that allows firms to alter the terms and service level of consumers who refuse targeted advertising). In *Mainstream Marketing Services, Inc. v. Federal Trade Commission*, the Tenth Circuit Court of Appeals upheld the FTC's "Do Not Call" registry against a First Amendment challenge in large part because the registry was set up as an opt-in system, leaving telemarketers the ability to continue communicating with all potentially-willing listeners who did not opt into the Do Not Call list.[80]

If the Commission uses rulemaking to restrict or ban data collection generally, or to impede uses that are purely expressive (such as serving customized content or generating new information), the rule very likely will have to pass strict scrutiny.[81]

6. Failure to Engage the Empirical Evidence

The Commission should consider sound empirical evidence when considering whether to issue a proposed rule that could potentially remake a substantial part of the US economy. The FTC's Bureau of Economics (BE) comprises approximately 80 of the leading consumer protection and competition economists in the world, making the FTC extraordinarily well-

[78] 564 U.S. 552 (2011).
[79] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557 (1980).
[80] Mainstream Marketing Services, Inc. v. F.T.C., 358 F.3d 1228 (2004).
[81] *See* Florida Star v. B.J.F., 491 U.S. 524 (1989); Cohen v. California, 403 U.S. 15 (1971); Wollschlaeger v. Governor of Florida, 848 F.3d 1293, 1302–03 (11th Cir. 2017); Conant v. Walters, 309 F.3d 629, 637–38 (9th Cir. 2002).

positioned to produce its own empirical evidence and evaluate the relevant extant empirical literature. For example, BE has unrivaled experience in the economic analysis of online advertising, search, and social media markets, including its analysis of the Google-DoubleClick merger, the Google search investigation, the recent Facebook antitrust actions, as well as the high-profile privacy matters involving Facebook, Google, and YouTube.[82]

Yet, the overwhelming majority of sources (other than cases, statutes, regulations, or speeches) on which the ANPR relies are news media and law review articles.[83] Even more jarring, the ANPR cites *no* economic literature at all, even though the relevant literature is remarkably rich, and the FTC enjoys enormous in-house expertise. The decision to issue a rule as sweeping as the one suggested by the ANPR must rest on empirical evidence that can reliably isolate causal relationships, not anecdotes from media outlets and normative arguments from legal academics. To accomplish that goal, the FTC must utilize the Bureau of Economics to conduct its own analysis and to evaluate the extant empirical evidence and evidence provided by commenters.

7. Conclusion

Taken as a whole, the ANPR seems to expect an impossible set of business practices from the digital market. Firms are expected to refrain from selling or repurposing consumer data, but they are also expected to deliver low-price (or no-price), high-quality services. And they are expected to be in robust competition with each other (as well as new startups) despite the obvious advantage that incumbent firms will have over firms that cannot afford a significant privacy compliance apparatus and are unable to purchase or repurpose consumer data. The FTC's objectives—privacy and quality and variety of services—are in tension with each other to some degree and in some contexts, but the ANPR has been crafted to avoid discussion of this tension. Consumers will not be well-served unless the Commission digests the full range of evidence, acknowledges the significant gaps in knowledge, and is frank with the public about trade-offs.

The available empirical evidence suggests little reason to believe that consumers suffer widespread harm from the routine collection and use of data in the online commercial context. At the same time, the value to society created by this ecosystem is substantial. A departure from the current base-by-case application of Section 5, which targets specific unfair or deceptive practices that harm consumers, in favor of broad prohibitions on the collection and use of data suggested by the ANPR, is likely to do more harm than good. For this reason, we strongly urge the Commission to refrain from adopting a proposed rule.

---

[82] *See*, *e.g.*, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. 2019); F.T.C. v. Google, LLC, No. 1:19-cv-02642 (D.D.C. 2019); Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170 (2007).

[83] Our analysis of the ANPR suggests that media and law review articles together comprise approximately 65 percent of the unique sources cited, excluding cases, consent agreements, statutes, regulations, and speeches.