Comments of the International Center for Law & Economics

FTC Advance Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security

Docket No. FTC-2022-0053, Commercial Surveillance ANPR, R111004

November 21, 2022

Authored by:

Geoffrey A. Manne (President & Founder, International Center for Law & Economics)

Daniel Gilman (Senior Scholar, International Center for Law & Economics)

Kristian Stout (Director of Innovation Policy, International Center for Law & Economics)

Comments of the International Center for Law & Economics

November 2022

Geoffrey A. Manne, Daniel Gilman, & Kristian Stout*

Executive Summary

The Federal Trade Commission ("FTC") has issued an Advanced Notice of Proposed Rulemaking ("ANPR") on "Commercial Surveillance and Data Security,"[1] initiating a proceeding intended to result in binding rules regarding "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."[2]

There is reason to believe that streamlined and uniform federal data-security or privacy regulations could be both beneficial and within the FTC's competence and authority. But the approach suggested by the ANPR—simultaneously sweeping and vague—appears very likely to do more harm than good. Most notably, the ANPR evinces an approach that barely acknowledges either the limits of the FTC's authority or the tremendous consumer benefits produced by the information economy.

The FTC is uniquely positioned to understand the complexities entailed in regulating privacy and data security. It has expertise and experience in both consumer-protection and competition matters. With regard to privacy and data security, in particular, it has decades of experience bringing enforcement actions for violations of the FTC Act's prohibition of deceptive and unfair practices. Its enforcement experience also has been bolstered by its statutory mission to conduct economic and policy research, which has, not incidentally, comprised numerous hearings, workshops, studies, and reports on issues pertinent to data policy.

The ANPR does not build on the Commission's experience and expertise as it could, however, and its dearth of economic analysis is especially striking. Moreover, the Commission's authority is not unbounded, and neither are its resources. Both limitations are salient when the Commission considers adopting substantive—or "legislative"— regulations under either Section 18 or Section 6 of the FTC Act. As we discuss below, the current proceeding is deficient on both substantive and procedural grounds. Absent an express grant of authority and the requisite resources from Congress, the

---

* Geoffrey A. Manne is the president and founder of the International Center for Law & Economics (ICLE). Daniel Gilman is a senior scholar with ICLE. Kristian Stout is ICLE's director of innovation policy.

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FED. REG. 51273 (Aug. 22, 2022) (to be codified at 16 C.F.R. Ch. 1) [hereinafter "ANPR" or "Commercial Surveillance ANPR"].

[2] *Id.* at 51277.

Commission would be ill-advised to consider, much less to adopt, the kinds of sweeping data regulations that the Commercial Surveillance ANPR appears to contemplate.

A. The FTC Must Provide More Detail Than Is Contained in the ANPR

The ANPR states that it was issued pursuant to the Commission's Section 18 authority,[3] which both grants and restrains the FTC's authority to adopt regulations with respect to "unfair or deceptive acts or practices in or affecting competition" ("UDAP").[4] Rulemaking under Section 18 of the FTC Act[5] requires that the Commission follow a careful process. As a preliminary matter, it must identify for both Congress and the public an area of inquiry under the Commission's jurisdiction; the Commission's objectives in the rulemaking; and regulatory alternatives under consideration.[6] Unfortunately, the Commission has not met these obligations in this ANPR.

Under Section 18, the Commission may adopt "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce"[7] under Section 5 of the FTC Act. Section 18 imposes express procedural requirements, in addition to those set out for this ANPR. These include, but are not limited to, requirements for a Notice of Proposed Rulemaking ("NPRM"). Section 18 also incorporates by reference the procedures prescribed by the Administrative Procedure Act.[8]

As noted, Section 18's requirements for an ANPR are brief and preliminary but they are nonetheless real. In contravention of the requirements of Section 18, this ANPR does not clearly describe any "objectives which the Commission seeks to achieve," and it provides no indication of "possible regulatory alternatives under consideration by the Commission."[9] Instead, it provides a laundry list of putative harms, and it fails to identify even the most basic benefits that may be associated with diverse commercial-data practices. It does not describe the Commission's current assessment of, or position on, those practices. And it provides no sense of the direction the Commission intends to take regarding potential rules.

Failing to identify the Commission's objectives or proposals under consideration, this ANPR fails in its basic purpose to "invite… suggestions or alternative methods for achieving [the] objectives."[10]

---

[3] *Id.* at 51276.

[4] That is, "unfair or deceptive acts or practices in or affecting commerce," as they are prohibited under Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1).

[5] 15 U.S.C. § 57a.

[6] 15 U.S.C. § 57a(b)(2)(A).

[7] 15 U.S.C. § 57a(a)(1)(B).

[8] 15 U.S.C. § 57a(b)(1) ("When prescribing a rule under subsection (a)(1)(B) of this section, the Commission shall proceed in accordance with section 553 of title 5.")

[9] 15 U.S.C. § 57a(b)(2)(i).

[10] 15 U.S.C. § 57a(b)(2)(ii).

B. The Commission Must Undertake a Cost-Benefit Analysis that Defines Harms, Identifies Benefits, and Weights the Two

Any rules the Commission issues under a Section 18 proceeding must emerge from a cost-benefit analysis.[11] Both the potential harms *and the benefits* of challenged conduct must be well-defined, and they must be weighed against each other. Even at this early stage of the process, the FTC is obligated to provide more than a suggestion that some harm might be occurring, and to provide more than a hint of how it might handle those harms.

This is also good procedure for policymaking more generally, irrespective of the Commission's statutory obligations under Section 18. Before engaging in a deeply interventionist regulatory experiment—such as imposing strict privacy regulations that contravene revealed consumer preferences—the Commission should publicly state empirically justified reasons to do so. In other words, there should be demonstrable market failures in the provision of "privacy" (however we define that term) before centralized regulation co-opts the voluntary choices of consumers and firms in the economy, and before it supplants the ability to redress any residual, cognizable harms through law enforcement with broad, economywide, *ex ante* rules.

Thus, a vital threshold question for any rules issued under this proceeding is whether and why markets operating without specific privacy regulation generate a suboptimal provision of privacy protection. Without this inquiry, it is unclear whether there are problems requiring regulatory intervention and, if so, what they are. Without knowing their purpose, any rules adopted are likely to be ineffective, at best, and harmful, at worst. They may increase costs for consumers and businesses alike, chill innovation, mandate harmful prescriptions for alleged privacy harms while failing to address the most serious and persistent harms, or exacerbate the risks of harm—or all of the above.

Particularly in the United States, where informational privacy is treated both legally and socially as more of a consumer preference (albeit, perhaps, a particularly important one) than a fundamental right,[12] it is difficult to determine whether our current regime produces the "right" amount of privacy protection. That cannot be determined by observing that some advocates and consumers who are particularly privacy-sensitive opine that there should be more, or more of a certain sort; nor is it enough that there have been some well-publicized violations of privacy and cases of demonstrable harm. Indeed, the fact that revealed preferences in the market tend toward relatively *less* privacy protection is evidence that advocates may be seeking to create a level and a type of privacy protection for which there is simply no broad-based demand. Absent a pervasive defect that suggests a broad disconnect between revealed and *actual* preferences, as well as a pattern of substantial net harm, the Commission should be extremely cautious before adopting preemptive and sweeping regulations.

---

[11] *See* Section III, *infra* (regarding the role of cost-benefit analysis under Magnuson-Moss and the statutory requirements of Section 18).

[12] Except, of course, when it comes to *government* access to private information, *i.e.*, under the Fourth Amendment.

At a minimum, the foregoing indicates that the Commission must undertake several steps before this ANPR is close to satisfying the requirements of Section 18, not to mention good government:

- **First, the Commission must proffer an adequate definition of "commercial surveillance."** While the ANPR is framed around this ominous-sounding term,[13] it is functionally defined in a way that is both sweeping and vague. It appears to encompass virtually all commercial uses of "consumer data," albeit without providing a workable *definition* of "consumer data."[14] If the Commission is contemplating a general data regulation, it should say so and enumerate the objectives such a regulation would serve. In the current ANPR, the Commission has done neither.

- **Second, the Commission must do more than merely cite diverse potential harms arising from what it terms "commercial surveillance."** The Commission has a long history of pursuing privacy and data-security cases, and it should rely on this past practice to define with specificity the types of harms—cognizable as injuries under Section 5—that it intends to pursue.

  The Commission must also adequately account for the potential harms to innovation and competition that can arise from the *adoption* of new privacy and data-security regulations. Resources that firms invest in compliance cannot be invested in product development, customer service, or any of a host of other ends. And compliance with overly broad constraints will often curtail or deter the sort of experimentation that is at the heart of innovation.

  Moreover, there is a potential tension between privacy and data security, such that mandates to increase privacy can diminish firms' ability to ensure data security. The EU's experience with the General Data Protection Regulation ("GDPR") has demonstrated some of this dynamic.[15] These realities must be incorporated into the Commission's assessment.

- **Third, the Commission must do more than merely nod to potential benefits that the modern data-driven economy provides to consumers.** The clear benefits that arise from information sharing must be considered. Since the dawn of the Internet, free digital services have created significant consumer surplus. This trend continues today: Research using both survey and experimental methods has consistently found substantial benefits for consumers from sharing information in exchange for free (or subsidized) digital products. Moreover,

---

[13] *See, e.g.*, ANPR, *supra* note 1 at 51273-75.

[14] The purported definition of consumer data in the ANPR, and the scope of activities around consumer data, are so overbroad as to encompass virtually the entirety of modern economic activity: "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information. These data include both information that consumers actively provide—say, when they affirmatively register for a service or make a purchase—as well as personal identifiers and other information that companies collect, for example, when a consumer casually browses the web or opens an app. This latter category is far broader than the first." *Id.* at 51277.

[15] *See, e.g.*, Coline Boniface, *et al.*, *Security Analysis of Subject Access Request Procedures*, in PRIVACY TECHNOLOGIES & POLICY: 7TH ANNUAL PRIVACY FORUM (Maurizio Naldi, *et al.* eds., 2019).

productive conduct and consumer benefits are not limited to free digital products and services. Myriad products and services—from health care to finance to education—are made more efficient, and more widely available, by the commercial use of various forms of consumer data.

C. The ANPR Must Account for the Effect of Any 'Commercial Surveillance' Rules on Consumer Welfare and Competition

The Commission is obligated to consider the likely effects of data regulation on consumers and competition. That ought to be a requirement for regulation generally, but it is an *express, statutory* requirement for unfairness regulation under Section 18 of the FTC Act. The Commission is uniquely well-situated to meet that mandate by virtue of its distinctive, dual competition and consumer-protection missions. Indeed, the Commission's antitrust-enforcement experience dates to the agency's inception. In addition, the Commission can access the considerable expertise of its Bureau of Economics, which employs experts in both industrial organization and consumer-protection economics. Yet much of that expertise appears absent from the ANPR.

This ANPR does not specify, or even sketch, the data regulations being contemplated by the Commission. Neither does it specify the Commission's goals in the rulemaking or alternative regulatory approaches under consideration, although both are required by statute. Consequently, one cannot assess the net effects of any proposed "commercial surveillance and data security" rule on competition or consumers, because there simply is no proposed rule to assess.

The economic literature, however, does suggest caution:

- First, as a general matter, regulations that impose substantial fixed costs on regulated firms tend to burden smaller firms and entrants more than they do large firms and incumbents.[16]
- Second, studies of specific domestic-privacy and data-security requirements underscore the potential for unintended consequences, including competitive costs.[17]
- Third, empirical studies of the effects of general data regulations in foreign jurisdictions, such as the EU's GDPR, suggest that such regulations have indeed led to substantial competitive harms.[18]

The literature on the effects of GDPR and other data regulations is particularly instructive. Although it is neither definitive nor complete, it has thus far found slender (at best) benefits to competition

---

[16] *See, e.g.*, James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47 (2015); Alex Marthews & Catherine Tucker, *Privacy Policy and Competition*, ECON. STUD. AT BROOKINGS (December 2019), *available at* https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf.

[17] *See, e.g.*, Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, 46 RAND J. ECON. 1 (2015).

[18] *See, e.g.*, Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-run Effects of the General Data Protection Regulation on Technology Venture Investment*, 40 MARKETING SCI. 661 (2021).

or consumers from data regulations and considerable costs and harms from their imposition. Further experience with and study of data regulations could yield a more nuanced picture. And, again, the FTC is well-positioned to contribute to and foster a greater understanding of the competitive effects of various types of data regulation. Doing so could be greatly beneficial to policymaking, competition, and consumer welfare, precisely because specific data practices can produce substantial benefits, harms, or a complex admixture of the two. But documented harms and speculative benefits of regulation recommend caution, not blind intervention.

D. Conclusion

The Commission should take account of a further reality: the rules it contemplates will be created in an environment filled with other privacy regulators. Although the United States does not have a single, omnibus, privacy regulation, this does not mean that the country does not have "privacy law." Indeed, generally applicable laws providing a wide range of privacy and data-security protections already exist at both the federal and state level. These include consumer-protection laws that apply to companies' data use and security practices,[19] as well as those that have been developed in common law (property, contract, and tort) and criminal codes.[20] In addition, there are sector-specific regulations pertaining to particular kinds of information, such as medical records, personal information collected online from children, and credit reporting, as well as regulations prohibiting the use of data in a manner that might lead to certain kinds of illegal discrimination.[21]

Despite the FTC's noted experience in a certain slice of privacy regulation, Congress has not made the FTC the central privacy regulatory body. Neither has Congress granted the Commission the resources likely required for such a regulator. Congress has wrestled with complex tradeoffs in several areas and has allowed—through design and otherwise—various authorities to emerge. Where Congress has provided for privacy regulation, it has tailored the law to address specific concerns in specific sectors, or with respect to specific types of information. Moreover, in each case, it has balanced privacy and security concerns with other policy priorities. That balancing requires technical

---

[19] *See, e.g.*, FTC Act, 15 U.S.C. § 45(a) et seq.

[20] *See Privacy-Common Law*, LAW LIBRARY—AMERICAN LAW AND LEGAL INFORMATION, http://law.jrank.org/pages/9409/Privacy-Common-Law.html (*last visited* Oct. 16, 2022).

[21] *See, e.g.*, Comments of the Association of National Advertisers on the Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, *available at* https://docplayer.net/93116976-Before-the-federal-trade-commission-washington-d-c-comments-of-the-association-of-national-advertisers-on-the.html:

> [T]he Health Information Portability and Accountability Act ("HIPAA") regulates certain health data; the Fair Credit Reporting Act ("FCRA") regulates the use of consumer data for eligibility purposes; the Children's Online Privacy Protection Act ("COPPA") addresses personal information collected online from children; and the Gramm–Leach–Bliley Act ("GLBA") focuses on consumers' financial privacy; the Equal Employment Opportunity Commission ("EEOC") enforces a variety of anti-discrimination laws in the workplace including the Pregnancy Discrimination Act ("PDA") and American with Disabilities Act ("ADA"); the Fair Housing Act ("FHA") protects against discrimination in housing; and the Equal Credit Opportunity Act ("ECOA") protects against discrimination in mortgage and other forms of lending.

Id. at 6.

expertise, but it also entails essentially political judgements about the relative value of diverse policy goals; in that latter regard, it is a job for Congress.

There are, as well, questions of resource allocation that may attend an express statutory charge. We cannot gainsay the importance of the FTC's privacy and data-security enforcement work under Section 5 of the FTC Act. At the same time, we cannot help but notice a misfit between the Commission's congressionally allocated resources and the obligations that are entailed by data regulations of the scope contemplated in the ANPR. By way of contrast, we note that, since the compliance date of the Health Insurance Portability and Accountability Act ("HIPAA") privacy rule, the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") has investigated and resolved nearly 30,000 cases involving HIPAA-covered entities and their business associates; for appropriate cases of knowing disclosure or obtaining of protected health information, OCR has referred more than 1,500 cases to the U.S. Department of Justice ("DOJ") for criminal prosecution.[22]

In his dissent from the issuance of this ANPR, former Commissioner Noah Phillips noted the massive and complicated undertaking it initiates:

> Legislating comprehensive national rules for consumer data privacy and security is a complicated undertaking. Any law our nation adopts will have vast economic significance. It will impact many thousands of companies, millions of citizens, and billions upon billions of dollars in commerce. It will involve real trade-offs between, for example, innovation, jobs, and economic growth on the one hand and protection from privacy harms on the other. (It will also require some level of social consensus about which harms the law can and should address.) Like most regulations, comprehensive rules for data privacy and security will likely displace some amount of competition. Reducing the ability of companies to use data about consumers, which today facilitates the provision of free services, may result in higher prices—an effect that policymakers would be remiss not to consider in our current inflationary environment.[23]

This is particularly true given the Commission's long history of work in this area. The Commission has undertaken decades of investigations and a multitude of workshops and hearings on privacy and related topics. This ANPR nods to that history, but it does not appear to make much use of it, possibly because much of it contains lessons that pull in different directions. Overall, that impressive body of work does not remotely point to the need for a single, comprehensive privacy rule. Rather, it has demonstrated that privacy regulation is complicated. It is complicated not just as a technical matter, but also because of the immense variety of consumers' attitudes, expectations, and preferences with respect to privacy and the use of data in the economy.

The Commercial Surveillance ANPR poses 95 questions, many of which will find some answers in this prior history if it is adequately consulted. The Commission has generally evidenced admirable

---

[22] Dep't Health & Human Servs., Health Information Privacy, Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (HHS Office of Civil Rights, *last reviewed* Sep. 14, 2022).

[23] ANPR at 51293 (Dissenting Statement of Comm'r Noah J. Phillips).

restraint and assessed the relevant tradeoffs, recognizing that the authorized collection and use of consumer information by companies confers enormous benefits, even as it entails some risks. Indeed, the overwhelming conclusion of decades of intense scrutiny is that the application of *ex ante* privacy principles across industries is a fraught exercise, as each industry—indeed each firm within an industry—faces a different set of consumer expectations about its provision of innovative services and offering of privacy protections.

These considerations all militate in favor of regulatory restraint by the FTC as a matter of policy. They also require restraint, and an emphasis on established jurisdiction, given the Supreme Court's recent "major questions" jurisprudence.[24] As noted in the statements of several commissioners, *West Virginia v. EPA*[25] clarifies the constitutional limits on an agency's authority to extend the reach of its jurisdiction via regulation. In brief, the broader the economic and political sweep of data regulations the Commission might propose, the more likely it is that such regulations exceed the FTC's authority. If the "major questions doctrine" is implicated, the burden is on the agency to establish the specific grant of authority that is claimed.[26] Moreover, the Court was clear that a merely colorable claim of statutory implementation is inadequate to establish the authority to issue sweeping regulations with major economic and political implications.[27]

[24] *See W. Virginia v. Env't Prot. Agency*, 142 S. Ct. 2587, 2595 (2022) (citing a line of cases including *Utility Air Regulatory Group v. EPA*, 573 U. S. 302 (2014); *Gonzales v. Oregon*, 546 U. S. 243 (2006); *FDA v. Whitman v. American Trucking Assns., Inc.*, 531 U. S. 457, 468 (2001); and *Brown & Williamson Tobacco Corp.*, 529 U. S. 120, 159 (2000)).

[25] *Id.*

[26] See *id.* at 2613 (*citing* WILLIAM ESKRIDGE, INTERPRETING LAW: A PRIMER ON HOW TO READ STATUTES AND THE CONSTITUTION 288 (2016)).

[27] *Id.* at 2608-09.

I. Introduction

The Federal Trade Commission ("FTC") has issued an Advanced Notice of Proposed Rulemaking ("ANPR") on "Commercial Surveillance and Data Security,"[1] initiating a proceeding intended to result in binding rules regarding "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."[2]

There is reason to believe that streamlined and uniform federal data-security or privacy regulations could be both beneficial and within the FTC's competence and authority. But the approach suggested by the ANPR—simultaneously sweeping and vague—appears very likely to do more harm than good. Most notably, the ANPR evinces an approach that barely acknowledges either the limits of the FTC's authority or the tremendous consumer benefits produced by the information economy.

The FTC is uniquely positioned to understand the complexities entailed in regulating privacy and data security. It has expertise and experience in both consumer-protection and competition matters. With regard to privacy and data security, in particular, it has decades of experience bringing enforcement actions for violations of the FTC Act's prohibition of deceptive and unfair practices. Its enforcement experience also has been bolstered by its statutory mission to conduct economic and policy research, which has, not incidentally, comprised numerous hearings, workshops, studies, and reports on issues pertinent to data policy.

The ANPR does not build on the Commission's experience and expertise as it could, however, and its dearth of economic analysis is especially striking. Moreover, the Commission's authority is not unbounded, and neither are its resources. Both limitations are salient when the Commission considers adopting substantive—or "legislative"— regulations under either Section 18 or Section 6 of the FTC Act. As we discuss below, the current proceeding is deficient on both substantive and procedural grounds. Absent an express grant of authority and the requisite resources from Congress, the Commission would be ill-advised to consider, much less to adopt, the kinds of sweeping data regulations that the Commercial Surveillance ANPR appears to contemplate.

II. The Central Role of Cost-Benefit Analysis Under Magnuson-Moss Rulemaking

The ANPR's breadth and lack of specificity challenge the basic statutory requirements of Section 18. First, while an ANPR does not yet have to specify "with particularity the text of the [proposed] rule, including any alternatives," it does require a description of, among other things, the "objectives the Commission seeks to achieve, and possible regulatory alternatives under consideration by the

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FED. REG. 51273 (Aug. 22, 2022) (to be codified at 16 C.F.R. Ch. 1) [hereinafter "ANPR" or "Commercial Surveillance ANPR"].

[2] *Id.* at 51277.

Commission."[3] A sweeping scope of inquiry, with key terms undefined, is not conducive to a clear statement of purpose or objectives, and a laundry list of domestic and foreign privacy and data-security laws and regulations[4] is not a clear statement of regulatory alternatives. Second, as we discuss in more detail below, the Magnuson-Moss amendments to the FTC Act underscore the key role of cost-benefit analysis—including consideration of competitive effects—in Section 5 consumer-protection enforcement and regulation. Yet the ANPR's treatment of harms to consumers, benefits of challenged practices, and the weighing of the two is woefully insufficient.

A. Basic Requirements of Magnuson-Moss Rulemaking

The ANPR states that it was issued "pursuant to Section 18 of the Federal Trade Commission Act ('FTC Act') and the Commission's Rules of Practice."[5] Section 18 of the FTC Act[6] both grants and restrains the Commission's rulemaking authority with respect to "unfair or deceptive acts or practices in or affecting competition" ("UDAP").[7]

Substantive rules adopted under Section 18—as opposed to the issuance of "interpretive rules and general statements of policy"—are, among other things, "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce"[8] under Section 5 of the FTC Act. Section 18 also sets forth certain procedural and substantive requirements for such rules. As a Senate Commerce, Science, and Transportation Committee Report noted following subsequent amendments, the Section 18 amendments to the FTC Act were adopted to permit a more limited and restrained authority for UDAP rulemaking.[9] These followed, in no small part, from congressional oversight hearings finding that, "in many instances the FTC had taken actions beyond the intent of Congress"[10] and that, in at least one rulemaking, the "Commission apparently endorsed a broad and virtually unbounded definition of unfairness."[11] The report further criticized the initiation of an additional FTC rulemaking because a relevant FTC report had failed to "indicate a 'pattern' of violations," even as it had identified certain deficiencies in the prior standard-setting practices it sought to address.[12]

---

[3] 15 U.S.C. § 57a(b)(2)(A)(i).

[4] ANPR, *supra* note 1 at 51276-77 (Aug. 22, 2022).

[5] *Id.* at 51276.

[6] 15 U.S.C. § 57a.

[7] That is, "unfair or deceptive acts or practices in or affecting commerce," as they are prohibited under Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1).

[8] 15 U.S.C. § 57a(a)(1)(B).

[9] Federal Trade Commission Act of 1979, Report of the S. Comm, on Commerce, Science, and Transp. on S. 1991, together with Additional Views (96th Cong. 1979).

[10] *Id.* at 2.

[11] *Id.*

[12] *Id.* at 3.

The procedures for substantive Section 18 rulemaking include those imposed for administrative rulemaking more generally under the Administrative Procedure Act,[13] as well as additional procedures. Among other things, Section 18 requires that "[p]rior to the publication of any notice of proposed rulemaking… the Commission shall publish an advance notice of proposed rulemaking in the Federal Register." That ANPR must "contain a brief description of the area of inquiry under consideration, the objectives which the Commission seeks to achieve, and possible regulatory alternatives under consideration."[14]

Subsequent rulemaking may proceed under Section 18 only if the Commission determines, among other things, that unfair and deceptive acts are prevalent.[15] A determination of prevalence, in turn, requires that the Commission has "issued cease and desist orders regarding such acts or practices" or has other information indicating "a widespread pattern of unfair or deceptive acts or practices."[16] Having done so, the Commission may:

> (A) publish a notice of proposed rulemaking stating with particularity the text of the rule, including any alternatives, which the Commission proposes to promulgate, and the reason for the proposed rule; (B) allow interested persons to submit written data, views, and arguments, and make all such submissions publicly available; (C) provide an opportunity for an informal hearing in accordance with subsection (c); and (D) promulgate, if appropriate, a final rule based on the matter in the rulemaking record (as defined in subsection (e)(1)(B)), together with a statement of basis and purpose.[17]

Unfortunately, the ANPR fails to comply with these basic requirements under Magnuson-Moss. As the ANPR acknowledges,[18] the Magnuson-Moss amendments to the FTC Act also clarify the Commission's general consumer-protection authority under Section 5 of the FTC Act:

> The Commission shall have no authority under this section or [FTC Act Section 18] to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[19]

---

[13] 15 U.S.C. § 57a(b)(1) ("When prescribing a rule under subsection (a)(1)(B) of this section, the Commission shall proceed in accordance with section 553 of title 5.")

[14] 15 U.S.C. § 57a(b)(2)(A).

[15] *Id.* at § 57a(b)(3).

[16] 15 U.S.C. § 57a(b)(1).

[17] *Id.*

[18] 87 FED. REG. 51278 (regarding statutory unfairness standard).

[19] 15 U.S.C. § 45(n). These are requirements for "unfairness," which seems central to an undertaking of this scope. The Commission also notes, *id.*, that actionable deception must be material; that is, that it must be one that "would likely affect the consumer's conduct or decision with regard to a product or service."

Thus, the plain language of the FTC Act implies a balancing of costs and benefits. For purposes of regulation or statutory enforcement of the unfairness prohibition, the Commission must analyze costs (prohibited conduct is only that which "causes or is likely to cause substantial injury to consumers which is not reasonably avoided by consumers themselves") and benefits "to consumers or competition"; and the Commission "shall have no authority" where the costs are "outweighed by countervailing benefits."

B. The Commission Must Define 'Commercial Surveillance'

The ANPR's area of inquiry is unclear. "Commercial surveillance" is a highly suggestive term, but not one defined in laws or regulations already enforced by the Commission. It is not—so far as we know—defined in other federal laws; has not been developed in the Commission's Section 5 enforcement actions regarding, *e.g.*, privacy and data-security enforcement; and has not—so far as we know—been the subject of substantial agency guidance. Instead, in an apparent effort to imbue its area of inquiry with immense scope and gravity, the ANPR appears to define a new term of art, "commercial surveillance," as follows:

> the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information. These data include both information that consumers actively provide—say, when they affirmatively register for a service or make a purchase—as well as personal identifiers and other information that companies collect, for example, when a consumer casually browses the web or opens an app. This latter category is far broader than the first.[20]

That definition sweeps extremely broadly, potentially encompassing any commercial use of data that is—in some sense unspecified in the ANPR—"consumer data," together with the also undefined "direct derivatives of that information." Is "consumer data" coextensive with personally identifiable information ("PII") or sensitive personal information ("SPI") or some particular definition of PII or SPI? The ANPR does not say. And at least one of the ANPR's enumerated questions for comment poses a related question:

> Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?[21]

The ANPR cites disparate examples of commercial surveillance, ranging across, as the Commission observes, "the most basic aspects of modern life."[22] The plain language of the stipulated definition

[20] *Id.* at 51277.

[21] *Id.* at 51281.

[22] *Id.* at 51273.

of "commercial surveillance" is at once sweeping and vague. Moreover, it suggests an area of inquiry for which the term "surveillance" is both inapt and needlessly pejorative.[23]

For example, if a physician practice provides a patient portal so that health-care consumers can voluntarily input details of their health history into a secure electronic health records ("EHR") system, that practice—a commercial enterprise subject to Section 5 of the FTC Act—is collecting, retaining, and perhaps analyzing or transferring protected health information. Such collection and use may suggest concerns in addition to benefits. Indeed, it is conduct regulated under, *inter alia*, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and implementing regulations enforced by the U.S. Department of Health and Human Services ("HHS"), including the HIPAA privacy and data-security rules, the HHS information-blocking rule, etc.[24] Surely, sensitive patient-health information counts as "consumer data" if anything does. Still, given the many productive and consumer-welfare-enhancing uses of electronic-health information, it would be odd and potentially misleading to deem that conduct "surveillance" and imbue it with an inherently pejorative connotation.

One might raise analogous points about any number of information-processing practices. While materially deceptive advertising might rightly be subject to Section 5 enforcement actions—depending on facts and circumstances, it may be a harmful species of commercial fraud—the Commission has, for decades, recognized the importance of truthful and non-misleading advertising to consumer welfare. For example, in 1975, the FTC brought its landmark antitrust case against the American Medical Association's "ethical" restrictions on truthful and non-misleading price and service terms. The 2nd U.S. Circuit Court of Appeals affirmed the Commission's holding that the so-called ethical principles had "prevented doctors and medical organizations from disseminating information on the prices and services they offer, severely inhibiting competition."[25] Not incidentally, the Supreme

---

[23] Indeed, the term cannot help but evoke the political and highly contentious scope of a popular progressive rallying cry that is decidedly and deeply critical of its subject. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019). For a critique of the overwrought connotations of this use of the term "surveillance," see Jim Harper and Neil Chilson, *The Semantics of "Surveillance Capitalism": Much Ado About Something*, AMERICAN ENTERPRISE INSTITUTE (December 2021), *available at* https://www.aei.org/research-products/report/the-semantics-of-surveillance-capitalism-much-ado-about-something:

> The phrase "surveillance capitalism" carries a lot of meaning. It signals to readers of Zuboff's book—and especially to nonreaders—the book's contents and the gist of her arguments. Arguably, the phrase has done more than the book has to coalesce a community opposed to the depredations of Big Tech. But it may not be accurate. "Surveillance capitalism" exaggerates the power dynamics in today's information economy. It is a powerful use of language, however, implying that current conditions are a sociopolitical horror by combining two semantically charged words.

[24] Regarding HHS enforcement of the HIPAA privacy rule, *see* Dep't Health & Human Servs., Health Information Privacy, Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (*last visited* Sep. 14, 2022). Some matters implicate overlapping jurisdiction and, on occasion, parallel enforcement actions. *See, e.g.*, Fed. Trade Comm'n, *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Consumers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations* (Feb. 18, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial-privacy-customers-employeescvs (describing behavioral remedies under FTC order and referring to monetary payment to settle HIPAA enforcement by Dep't Health and Human Servs.).

[25] *American Medical Ass'n, v. FTC*, 638 F.2d 443 (2d Cir. 1980) (*aff'd* 455 U.S. 676).

Court's First Amendment jurisprudence recognizes the public interest in commercial speech, such as advertising: "It is a matter of public interest that [economic] decisions, in the aggregate, be intelligent and well-informed. To this end, the free flow of commercial information is indispensable."[26] As the Commission observed in its Policy Statement on Unfairness, "the agency has referred to First Amendment decisions upholding consumers' rights to receive information, for example, to confirm that restrictions on advertising tend unfairly to hinder the informed exercise of consumer choice."[27]

The ANPR raises several questions about the value of targeted advertising.[28] Digital advertising that incorporates some types of consumer information may, in particular instances, raise concerns analogous to those raised in other advertising matters. But it may also provide—and in some cases multiply—the benefits long recognized under the FTC Act and the First Amendment. While we lack a complete picture of the costs and benefits of digital advertising, there is considerable empirical evidence of its substantial positive value. For example, Goldfarb & Tucker studied the impact of the EU's Privacy and Electronic Communications Directive,[29] which imposed restrictions on the ability to collect user data and target advertising. The study examined the performance of advertising in EU member states that enacted it relative both to ad performance in Europe prior to the directive and to performance in nations without the directive's restrictions.[30] They found that, on average, ads became less effective relative to their performance in nations without the directive's restrictions. Moreover, they found the effect was greater for websites with general content, such as news sites, and for ads with a smaller presence on those websites.

In a separate study, Goldfarb & Tucker used data from a large-scale field experiment to examine the effects of both ad targeting and obtrusiveness.[31] They found that targeting increased effectiveness substantially, while the combination of targeting and ad obtrusiveness was not effective. More recently, Laub, Miller, & Skiera studied the impact of tracking by analyzing 42 million ad impressions from 100 publishers.[32] They found a 24% decrease in value without tracking, after controlling for differences in users, advertisers, and publishers.

---

[26] *Virginia Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748 (1976); *see also Central Hudson Gas & Elec. v. Public Svc. Comm'n*, 447 U.S. 557 (1980).

[27] Statement of Basis and Purpose, Advertising of Ophthalmic Goods and Services, 43 FED. REG. 23992,24001 (1978), *citing Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council,* 425 U.S. 748 (1976).

[28] 87 FED. REG. 51283 (enumerated questions 39-42).

[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[30] Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57.1 MGMT. SCI. 57 (2011).

[31] Avi Goldfarb & Catherine C. Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MKTG. SCI. 389 (2011).

[32] Rene Laub, Klaus Miller, & Bernd Skiera, *The Economic Value of User Tracking for Publishers*, SSRN Working Paper 4251233 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4251233.

While one working paper that examined the websites of a single media company found a small-but-positive value derived from cookies,[33] numerous other studies—including one conducted by a former director of the FTC's Bureau of Consumer Protection—find substantial value associated with cross-site identifiers and targeted advertising.[34]

Research also suggests the value of "cookies" and targeted ads is shared between advertisers, ad tech intermediaries, and publishers. Goldfarb & Tucker[35]—as well as Laub, *et al.*[36]—find outsized harmful effects for news and other general-content websites from the loss of cookies and targeted ads.

It would appear inapt to generically deem such diverse conduct to be "surveillance." Indeed, nearly any commercial conduct involving personally identifiable information or its "direct derivates" would seem to fit the definition put forth here. As the ANPR notes, such information is involved in buying groceries, doing homework, or applying for health insurance.[37] If the Commission is contemplating a general data regulation, it should say so—and enumerate the objectives such a regulation would serve. In the current ANPR, the Commission has done neither.

By taking such an expansive view of its regulatory subject, the Commission has seriously complicated its ability to comply with its obligations under Magnuson-Moss. As noted above, the Commission is obligated to describe not just regulatory objectives but possible regulatory alternatives under consideration. The Commission has not done so. Moreover, the capacious scope of the ANPR stands as an obstacle to meeting that obligation. If all commercial use of "consumer data" may be swept into this rulemaking, then regulatory alternatives are not simply missing, but innumerable. Alternatives might include personally identifiable information, sensitive personal information, or some other conception of "consumer information"—as well as "direct derivatives" of such information, whatever they may be. Alternatives might range across all such information or some silo or subset of it, whether sector-specific or issue-specific or otherwise. And restrictions could pertain to the collection, storage, analysis, or distribution of commercial data, or everything and anything a firm might do with that

---

[33] Veronica Marotta, Vibhanshu Abhishek, & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, Workshop on the Econ. of Info. Sec. Working Paper (2019), https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf (observing a 4% effect on one model). Curiously, the ANPR cites this research indirectly, though a newspaper article that discusses the working paper. 87 FED. REG. 51274 at n. 11. That indirect citation is supposed to support what is—a qualification of "may" notwithstanding—plainly an overgeneralization at best, and one that ignores the larger body of research in favor of a newspaper's gloss on a single working paper study of a single media firm's sites.

[34] J. Howard Beales & Jeffrey A. Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, Navigant Econ. Technical Report (2014), https://digitaladvertisingalliance.org/sites/aboutads/files/files/DAA_images/fullvalueinfostudy%20-%20Navigant.pdf (finding a 66% drop in value without cookies. Beales is a former director of the FTC's Bureau of Consumer Protection); *see also*, Garrett A. Johnson, Scott Shriver, & Shaoyin Du, *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, 39 MKTG. SCI. 33 (2020) (52% drop without cookies). Note that, while Laub, Miller & Skiera, *supra* note 32, found a 24% drop after adjusting for users, advertisers, and publishers, they observed a 60% drop in raw mean value.

[35] Goldfarb & Tucker, Online Display Advertising, *supra* note 31.

[36] Laub, Miller & Skiera, *supra* note 32.

[37] 77 FED. REG. 51273.

data. That alone should suggest to the Commission that the ANPR has fundamental flaws, and that it must more carefully and narrowly define the scope of its concerns to identify the particular problematic uses of data it wishes to address, and the particular harms it seeks to mitigate.

C. Conducting a CBA Means that Benefits Must Be Assessed

Trivially, cost-benefit analysis requires attention to actual and likely benefits, as well as harms, but the ANPR's treatment of such benefits is radically attenuated. The imbalance is especially baffling given the Commission's experience and expertise in competition matters generally, and in view of the statutory limits to the Commission's UDAP authority. The ANPR briefly acknowledges that diverse commercial practices dependent on personal data "in theory . . . have the potential to benefit consumers."[38] By way of contrast, actual and potential harms are discussed in the ANPR's "overview" section, and in the first 23 of the ANPR's 95 enumerated questions regarding diverse harms—within and without the ambit of Section 5, clear and vague, material and otherwise—that may be associated with commercial data practices.[39] The ANPR also raises several questions about balancing "the relative costs and benefits of any current practice, as well as those for any responsive regulation."[40] Benefits blithely acknowledged as merely "in theory" and made no more concrete than relating to the undifferentiated mass "of any current practice" are entirely out of balance with the ANPR's recitation of, and musings on, harms. More than that, the failure to discuss or sketch the family of benefits at issue is part and parcel with the Commission's failure to provide an adequate description of the domain of conduct at issue.

Setting forth the benefits and costs of allegedly unfair conduct is a statutory requirement for Section 18 rulemaking. As Congress made express in amending Section 5 of the FTC Act:

> The Commission shall have no authority under this section or [FTC Act Section 18] to declare unlawful an act or practice on the grounds that such act or practice is unfair **unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition**. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[41]

The Commission committed in its Unfairness Statement that it "will not find that a practice unfairly injures consumers unless it is injurious in its *net* effects."[42] But the "commercial surveillance" regime

---

[38] 87 FED. REG. 51274.

[39] *Id.* at 51281-82.

[40] *Id.* at 51282. Specifically, the ANPR raises two questions about the potential impact of data regulations on competition, *id.* at 5182-83, and two about potential *harm* to competition stemming from commercial data practices, *id.* at 51283-843.

[41] 15 U.S.C. § 45(n) (emphasis added).

[42] *In re Int'l Harvester Co.*, 104 F.T.C. 949, 1073 (1984) (emphasis added).

framed in the ANPR would overemphasize the risks of data possession by firms and fail to evaluate at all the constraints on innovation and experimentation.

There are clear benefits to information sharing that must be considered. Since the dawn of the Internet, free digital services have created significant consumer surplus. This trend continues today: Research using both survey and experimental methodologies has consistently found substantial benefits for consumers from sharing information in exchange for free (or subsidized) digital products.

Allcott, *et al.*, for example, studied the price that Facebook users were willing to accept in order to abstain from using the service for four weeks.[43] In the study, the median willingness to accept (WTA) from participants was $100.[44] The WTA estimate means that "[a]ggregated across an estimated 172 million US Facebook users, the mean valuation implies that four weeks of Facebook generates $31 billion in consumer surplus in the US alone."[45]

Corrigan, *et al.*, reported similar results of "a series of three non-hypothetical auction experiments where winners are paid to deactivate their Facebook accounts for up to one year."[46] In their conclusion, the researchers said: "Though the populations sampled and the auction design differ across the experiments, we consistently find the average Facebook user would require more than $1,000 to deactivate their account for one year."[47]

Brynjolfsson, *et al.* reviewed the benefits of "several empirical examples [of technology that implicates privacy concerns] including Facebook and smartphone cameras" and then "estimate[d] their valuations through incentive-compatible choice experiments."[48] The study found considerable benefits that are currently excluded from national accounts: "For example, including the welfare gains from Facebook would have added between 0.05 and 0.11 percentage points to GDP-B growth per year in the US."[49] And a 2018 study from the Federal Reserve Bank of Philadelphia analyzed the contribution of "free" content to domestic production; as a result, the authors estimated an addition of $294 billion to U.S. GDP.[50]

---

[43] Hunt Allcott, Luca Braghieri, Sarah Eichmeyer, & Matthew Gentzkow, *The Welfare Effects of Social Media*, NBER Working Paper No. 25514 (2019).

[44] *Id.* at 5. Note, this was not just cheap talk—the study followed through and paid a randomly selected portion of the users to deactivate their accounts for four weeks. *Id.*

[45] *Id.*

[46] Jay R. Corrigan, *et al.*, *How Much Is Social Media Worth? Estimating the Value of Facebook by Paying Users to Stop Using It*, PLOS ONE (2018).

[47] *Id.*

[48] Erik Brynjolfsson, *et al.*, *GDP-B: Accounting for the Value of New and Free Goods in the Digital Economy*, NBER Working Paper No. 25695 (2019).

[49] *Id.*

[50] Leonard Nakamura, *et al.*, *"Free" Internet Content: Web 1.0, Web 2.0, and the Sources of Economic Growth*, Fed. Reserve Bank of Philadelphia Working Papers, WP 18-17 (2018), https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-17.pdf.

Indeed, a more thoroughgoing and consistent incorporation of cost-benefit analysis in privacy matters is an area where the Commission's past practice can be improved, the contributions and capabilities of the Commission's economics staff notwithstanding. In fact, staff from the FTC's Bureau of Economics outlined an approach to assessing consumer harm that could be applied to matters such as *Wyndham*, where the alleged harms included both direct financial losses and time spent to remedy those losses and guard against future ones.[51] Other research by FTC staff suggests that some difficulties in observation, measurement, and ordering are not necessarily intractable or permanent.[52] While this type of research is neither settled nor comprehensive, it does suggest a way forward as an alternative—or at least prologue—to regulation. But particularly in the context of data security, the Commission has avoided taking seriously the thoroughness of the required investigation and analysis sufficient to determine whether the costs (*i.e.*, foregone benefits) of incremental increases in harm avoidance are merited.[53]

In its Privacy Report, for instance, the Commission said that "[i]n terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace."[54] In other words, there are costs to potential data-security requirements and there are benefits, but because *some* benefit exists from the data-security requirements, the magnitude of the costs imposed by further regulation do not matter. As Commissioner Rosch pointedly noted, dissenting from the FTC Privacy Report:

> There does not appear to be any… limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world. That is not only paternalistic, but it goes well

---

[51] *See* Dan Hanner, Ginger Zhe Jin, Marc Luppino & Ted Rosenbaum, *Economics at the FTC: Horizontal Mergers and Data Security*, 49 REV. INDUS. ORG. 613, 627-30 (2016) (containing a discussion estimating harm from data breaches with application to *Wyndham*). The approach considers the estimated baseline rate of identity theft, conditional on a consumer's being subject to a breach. Because the Section 5 violation was predicated on the firm's deceptive statements, the FTC Bureau of Economics staff also estimated the price premium that consumers paid due to those deceptive statements, multiplied by an estimate of the number of consumers affected. The relief actually obtained in the matter was not monetary but behavioral, comprising a comprehensive information-security program, annual information-security audits, and other safeguards.

[52] Pappalardo, for instance, points to positive contributions of FTC economists, through a combination of research, case evaluation, and policy analysis, to the definition and estimation of consumer harms or injuries from deceptive or unfair practices, including those associated with lapses in data security or privacy protections. Janis K. Pappalardo, *Economics of Consumer Protection: Contributions and Challenges in Estimating Consumer Injury and Evaluating Consumer Protection Policy*, 45 J. CONSUMER POL'Y 201 (2022). She also describes a framework for estimating injury from deception using a combination of methods, such as consumer copy testing and comparative-demand analysis, that have been applied in such matters. *Id.*

[53] *See* Geoffrey A. Manne & Kristian Stout, *When Reasonableness Isn't: The FTC's Standardless Data Security Standard*, 15 J. LAW, ECON. & PUB. POL'Y 67 (2018) for further discussion.

[54] FTC, *Protecting Consumer Privacy in an Era of Rapid Change; Recommendations for Business and Policymakers*, at 8 (March 2012) [hereinafter "*FTC Privacy Report*"], *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

> beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[55]

The Commission's *Apple* product-design case is instructive of where the FTC's past practice can be improved concerning the inclusion of both benefits and costs in its evaluation of challenged conduct.[56] In that matter, the Commission brought charges against Apple for allegedly designing the iOS app store in a way that led to "unfair" billing practices. Historically, the Commission would bring such cases where a defendant affirmatively endeavored to mislead consumers—including cases of outright fraud, unauthorized billing, and cramming.[57] In the *Apple* case, however, the Commission alleged not that Apple engaged in irredeemably bad conduct, but rather that it had designed the App Store in a way that made it too easy for children to make purchases without parental consent[58] by permitting password-free purchases and downloads during a 15-minute window once a user had entered her password.[59]

This case highlights a crucial part of the FTC's mandate embodied in Section 5(n) that is all too frequently ignored: a likely harm can be deemed "unfair" only if there are insufficient countervailing benefits from the challenged practice, and if consumers could not themselves reasonably avoid the harm.[60] But in *Apple*, the FTC did not evaluate the potentially broad benefits of Apple's design decisions and essentially replaced its own judgment for that of Apple's—a company whose very existence depends on it making products for which consumers are willing to pay.

In other words, the Commission completely failed to perform an adequate analysis to determine if the "harm" suffered by the relatively small number of parents of children who were able to make a purchase within the 15-minute window was counterbalanced by the greater degree of convenience that an overwhelming number of consumers enjoyed by virtue of the feature. Moreover, scant attention was paid to assessing whether parents themselves were unable to avoid the potential harm, despite the likelihood of their proximity to their phones and their children.

And even where the Commission has conceded possible benefits from a firm's risk-increasing conduct, it often does so insufficiently. In its *LabMD* opinion, for instance, the Commission states that:

> A "benefit" can be in the form of lower costs and then potentially lower prices for consumers, and the Commission "will not find that a practice unfairly injures consumers unless it is injurious in its net effects."... This cost-benefit inquiry is particularly important in cases where the allegedly unfair practice consists of a party's failure to take actions that would prevent consumer injury or reduce the risk of such injury.... When a

---

[55] *Id.* at C-5 (J. Thomas Rosch, Comm'r, dissenting).

[56] *In re Apple Inc.*, 112-31008, 2014 WL 253519, at *1 (MSNET Jan. 15, 2014), https://www.ftc.gov/system/files/documents/cases/140327applecmpt.pdf.

[57] *See generally id.*

[58] *Id.* at 1.

[59] *Id.* at 5.

[60] 15 U.S.C. § 45(n) (1914)

> case concerns the failure to provide adequate data security in particular, "countervailing benefits" are the foregone costs of "investment in stronger cybersecurity" by comparison with the cost of the firm's existing "level of cybersecurity."... [W]e conclude that whatever savings LabMD reaped by forgoing the expenses needed to remedy its conduct do not outweigh the "substantial injury to consumers" caused or likely to be caused by its poor security practices.[61]

That breezy conclusion is questionable in a case where there was no breach, no assessment of direct consumer harm, and no estimate of the risk of consumer harm.[62] In addition, the Commission's construction assumed that the inquiry into countervailing benefits was strictly limited to the direct costs and benefits of the data-security practices themselves. That cannot be correct. The potential benefits to consumers are derived from the business (or product) as a whole, and the data-security practices are just one component of that. The proper tradeoff does not simply keep those benefits fixed while adding the direct costs of some specific data-security practices deemed to be lacking. In any given case, such costs might be substantial or trivial once a specific deficiency or vulnerability has been identified. But there are costs to assessing the firm's data-security practices *ex ante*. Absent clear regulatory standards, there are also costs, including uncertainty costs, to estimating those practices that would be deemed "reasonable," assessing the delta between extant and reasonable data-security tools and practices, and to planning improvements *ex ante*. There may be ongoing research, legal, and management costs. More broadly, there are the opportunity costs that a business faces when it seeks to further a certain set of aims—chief among them, serving customers—with limited resources.[63]

Analogous challenges face a would-be regulator. The Commission needs to account for how a privacy regulation that creates requirements that either make some business practices more difficult or impossible—or else layer on additional costs—affects the viability and operation of the firm as a whole. Privacy regulations do not operate in a vacuum. Restricting how and when firms can collect and use data can affect myriad endeavors—everything from the potential for a new entrant to challenge digital firms online to the viability of local retailers' use of loyalty programs that require gathering data on their shoppers.

Indeed, many or most of the innovative uses of data are unforeseeable *ex ante*. For example, earlier this year, Macy's executives noticed an uptick in how much consumers were spending on food and gas—the result of rising inflation—on the company's co-branded credit cards that shoppers can use at other retailers.[64] They also detected a shift as consumers began spending more on travel and

---

[61] LabMD, Inc., Docket No. C-9357 at 26 (FTC Jul. 29, 2016).

[62] *See generally* Manne & Stout, *supra* note 53.

[63] For further discussion of this point, *see* Manne & Stout, *supra* note 53, at 69.

[64] *See* Suzanne Kapner, *How Macy's Has Avoided–So Far–the Inventory Pileup Plaguing Other Apparel Chains*, WALL ST. J. (Oct. 5, 2022), https://www.wsj.com/articles/how-macys-has-avoidedso-farthe-inventory-pileup-plaguing-other-apparel-chains-11664930492.

entertainment outside the home.[65] Combining these insights, Macy's was able to tailor the kinds of goods it produced and sold, thereby avoiding the inventory glut suffered by many other retailers in the last year.[66] This greater efficiency translates into Macy's having greater ability to meet consumer demand, as well as to keep prices down amid inflationary pressures. Arguably, this would fit within the definition of "consumer surveillance" as the Commission broadly defines in in the ANPR. But just as arguably, this is exactly the kind of conduct that can help consumers through difficult economic times.

Not only are innovative uses of data difficult to predict, but understanding how consumers will value those innovations is likewise difficult because of heterogeneous preferences. In a literature review of the economics of privacy, Acquisti, *et al.*, concluded that:

> Extracting economic value from data and protecting privacy do not need to be antithetical goals. The economic literature we have examined clearly suggests that the extent to which personal information should be protected or shared to maximize individual or societal welfare is not a one-size-fits-all problem: **the optimal balancing of privacy and disclosure is very much context-dependent, and it changes from scenario to scenario**.[67]

D. The Required Cost-Benefit Analysis Requires Well-Defined Harms

Briefly describing or citing diverse potential harms, the ANPR states that it "has alluded to only a fraction of the potential consumer harms arising from lax data security or commercial surveillance practices, including those concerning physical security, economic injury, psychological harm, reputational injury, and unwanted intrusion."[68] That may be true. Past Commission enforcement actions assess and address real consumer harms—including, but not limited to, financial harms.[69] Still, that leaves the scope of the Commission's concern unclear. Nothing in the ANPR cabins the area of inquiry further than what appears to be a diverse, if not discursive, laundry list of potential harms associated with conduct constitutive of much of the digital economy; that is, with the collection, storage, processing, and distribution of "consumer data" and their derivatives.

---

[65] *Id.*

[66] *Id.*

[67] Alessandro Acquisti, Curtis R. Taylor, & Liad Wagman, *The Economics of Privacy*, 52 J. ECON. LIT. 48 (2016) (emphasis added).

[68] *Id.* at 51281.

[69] In *Wyndham*, for example, substantial losses of consumer time spent addressing ID theft, in addition to monetary losses, were associated with a sequence of three major data breaches. In *EMP Media*, the FTC and state enforcers together alleged that the firm's website, MyEx.com, was dedicated solely to revenge porn, violating federal and state law by posting intimate images of people, together with their personal information, such as the name, address, employer, email address, and social-media account information, without consent. *FTC v. Emp Media, Inc.*, 2018 U.S. Dist. LEXIS 16463, 5-6 (D. Nev. 2018) (complaint for permanent injunction and other equitable relief). Victims were subject to threats, harassment, and the loss of employment and, in numerous instances, the defendants allegedly charged victims fees from $499 to $2,800 to remove their images and information from the site. *Id.* at 14-17.

Independent of the question of the magnitude and distribution of such harms, and of what conduct might be harmful on net, we note that many of the harms are simply undefined. To be sure, some of these harms are clear enough and some are subject to straightforward measurement. But the scope and vagueness of the collected set of harms mentioned in the ANPR—"only a fraction of the potential consumer harms arising from lax data security or commercial surveillance practices, including those concerning physical security, economic injury, psychological harm, reputational injury, and unwanted intrusion"[70]—are fundamentally at odds with the statutory requirement that UDAP rulemaking address "a widespread pattern of unfair or deceptive acts or practices."[71] If both the conduct and the harms at issue are open-ended, what guides or constrains identification of a pattern?

The need for specificity here is not driven solely by the relevant statutory requirements, but also by the ambiguity in how consumer-protection law should treat privacy, data, and data breaches. When there is a breach—an exposure of private data—calculating the magnitude of informational harm (if any) to consumers is often difficult. This is complicated, of course, by the often tenuous or uncertain connection between conduct and injury. To use the language of tort law, establishing "proximate cause" can be challenging or even intractable.[72]

Identification and assessment of harms is thus critical to Section 18 rulemaking, but that key project seems, at best, both fragmentary and nascent as the ANPR presents it. The lack of clarity seems especially puzzling given the substantial—and decades-long—enforcement, research, guidance, and advocacy resources that the Commission has devoted to privacy and data-security matters. For example, in 2017, the FTC hosted a workshop to discuss "informational injuries," which are injuries—both "market-based and non-market"—that consumers may suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[73] That workshop led to a brief staff paper that merely catalogued suggestions by invited workshop participants of four categories of potential "market and non-market informational injuries."[74] There was no suggestion that the taxonomy was comprehensive or even whether the Commission endorsed it. Between 1996 and 2022, the FTC and its staff published 24 reports on privacy, in addition to consumer education materials and industry guidance. Most recently, "Bringing Dark Patterns to Light" was issued the same month that the ANPR was published in the Federal Register.[75] As the ANPR notes, the Commission has brought

---

[70] 87 FED. REG. 51281.

[71] 15 U.S.C. § 57a(b)(1).

[72] *See* Manne & Stout, *supra* note 53.

[73] FTC, Informational Injury Workshop (Dec. 12, 2017), https://www.ftc.gov/news-events/events/2017/12/informational-injury-workshop.

[74] Fed. Trade Comm'n Staff, FTC Informational Injury Workshop, BE and BCP Staff Perspectives (2018), https://www.ftc.gov/news-events/events/2017/12/informational-injury-workshop.

[75] Fed. Trade Comm'n Staff, Bringing Dark Patters to Light (September 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf. While labeled a "Staff Report" rather than a "FTC Report," we note that publication of staff reports is typically contingent on an authorizing vote of the Commission, and that "the Commission voted 5-0 at an open meeting to authorize the release" of the "Dark Patterns" staff report. Fed. Trade Comm'n, *FTC Report Shows Rise in Sophisticated Dark*

"scores of enforcement actions concerning data privacy and security."[76] That substantial research and enforcement history should provide ample grounds for a much-needed synthesis. Besides an open-ended inquiry about perceived harms that may or may not be cognizable under the FTC Act, and prior to considering any general rulemaking, the Commission ought to clarify for both consumers and industry, as well as the Congress,[77] what it has learned about actionable informational injury and how the Commission intends to address it.

The 95 enumerated questions in the ANPR open with 23 regarding harms to consumers and harms to children, but the ANPR does not summarize the Commission's current understanding of actionable informational injuries. Recall the limits set forth in Section 5(n) of the FTC Act.[78] Deception enforcement (and regulation) depends upon materiality and unfairness enforcement (and regulation) requires an assessment of the costs and benefits of the conduct at issue. Identifying and assessing such harms is critical to that assessment. For that reason, and given the FTC's enforcement, research, education, and advocacy history, it strains credulity that the Commission might undertake a rulemaking regarding conduct that may cause informational harms or injuries without both having and presenting a more fully developed view of such injuries.[79]

Specific Section 5 *enforcement* matters that are somehow related to privacy or data security do not necessarily require a distinct theory of informational injury or, for that matter, a distinct domain of commercial conduct. For substantial harms caused by some course of conduct having to do with data or personal data, any cognizable injury under the FTC Act, in any area of commerce not expressly excepted from the FTC's jurisdiction, will do. Here, however, Section 18 requires that the Commission state the objectives it hopes to achieve by regulation. It has not done so. As

---

Patterns Designed to Trick and Trap Consumers, Press Release (Sep. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers.

[76] 87 FED. REG. 51278. We are unclear why the Commission has indicated "scores" of prior actions as, in prior statements, the Commission has noted that it has brought hundreds of cases and obtained billions in penalties to protect the privacy and security of consumer data. *See, e.g.*, Fed. Trade Comm'n, Privacy & Data Security Update for 2019, 1-2 (2020), https://www.ftc.gov/reports/privacy-data-security-update-2019 (noting, through calendar year 2019, more than 130 spam and spyware cases and 80 general privacy lawsuits, including a $5 billion settlement with Facebook, *id.* at 2; more than 75 data security cases, including a $375 million settlement with Equifax, *id.* at 5; more than 100 Fair Credit Reporting Act cases, *id.* at 7; close to 30 cases under the Children's Online Privacy Protection Act (COPPA) since 2000, *id.* at 8; about 35 cases under the Gramm- Leach-Bliley Act on financial institution privacy notices, *id.* at 7; and almost 150 cases enforcing do-not-call provisions, *id.* at 10). Although, of course, one can calculate hundreds as multiples of five.

[77] Section 18 also contemplates congressional oversight at the ANPR stage, requiring that the Commission submit the ANPR "to the Committee on Commerce, Science, and Transportation of the Senate and to the Committee on Energy and Commerce of the House of Representatives." 45 U.S.C. § 57a(b)(2)(B).

[78] *See supra* note 19, and accompanying text.

[79] A statement of the Commission's current understanding of informational injuries that are cognizable under Section 5 need not be final. There is nothing improper about asking whether an established standard is adequate. But if the Commission does not offer considerably more specificity than the ANPR provides, then the objectives of a potential rulemaking are left fundamentally unclear.

Commissioner Phillips noted in his dissent accompanying the ANPR, "[t]he areas of inquiry are vast and amorphous, and the objectives and regulatory alternatives are just not there."[80]

We believe that the FTC is well-positioned to issue guidance reflecting the Commission's current views of (a) privacy injury or harms, (b) data-security injury or harms, and/or (c) how the Commission's Section 5 "UDAP" authority applies to conduct causing or likely to cause privacy or data-security harms. But if the Commission cannot state more clearly what types of conduct are at issue, and what cognizable harms associated with that conduct are to be mitigated by a rule, then the public and Congress are left to guess at the nature and scope of the Commission's concerns and objectives—that is, at the very subject matter of this rulemaking.

E. Privacy and Data Security Policies Entail Complex Tradeoffs

1. Privacy is not a simple, valuable quality, but a complex array of preferences

Privacy is a complex matter, rather than a simple, qualitative measure of goods or services. Privacy policy is correspondingly complex. Some of the variation in privacy preferences is captured in the literature attempting to define privacy itself. In their landmark 1896 essay, Warren & Brandeis provided an extended meditation on privacy as a "right to be let alone."[81] Privacy has been described as an aspect or foundational element of dignity and autonomy,[82] as the control over or safeguard of personal information by the subject of that information,[83] and as the boundary between what is personal and that which is more widely shared,[84] and the decisions one can choose to make about those boundaries. Those decisions may entail complex tradeoffs concerning benefits and costs that are both tangible and intangible, under varying conditions of uncertainty, and with externalities that may vary along multiple dimensions. Prosser famously identified four "rather definite" privacy rights: intrusion upon a person's seclusion, solitude, or private affairs; public disclosure of embarrassing private facts about an individual; publicity placing one in a false light in the public eye; and appropriation of one's likeness for the advantage of another.[85] Solove reviewed six broad categories of conceptions of (or perspectives on) privacy: "(1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy."[86] Noting

---

[80] Fed. Trade Comm'n, Dissenting Statement of Commissioner Phillips Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking, 2 (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

[81] *See generally*, Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 5 (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT (1879)).

[82] *See* FERDINAND SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (1994).

[83] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

[84] *See* IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975).

[85] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[86] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1088, 1094 (2002); *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006) ("Many commentators have spoken of privacy as a unitary concept with a uniform value, which is unvarying across different situations. In contrast, I have argued that privacy violations involve a variety of types of harmful or problematic activities." *Id.* at 480).

difficulties with each of them, he suggested a "pragmatic" and context-dependent approach, rather than a particular theory or model.[87] Additional candidates are numerous and varied, as are rejections of the promise of a simple unified theory of privacy.[88]

Empirical research reinforces the notion that privacy is multi-dimensional and that privacy policies may entail complex tradeoffs. In early and influential survey-based research, Alan Westin used broad, non-context-specific privacy questions. Based on the results, he clustered individuals into privacy segments: privacy fundamentalists, pragmatists, and unconcerned.[89] Implicit in Westin's account was a distribution in the magnitude of consumer privacy preferences, if not necessarily a normal or smooth distribution. But Westin's clustering may be too crude—at least partly an artifact of the survey design—as consumers might fall into one or another category depending on context. Contextual variation also may depend on the domain of information at issue or any number of other factors.

Subsequent experimental research has suggested that many consumers attach relatively little value to at least certain types of privacy or privacy protections, and that behavioral evidence may be at odds with declared preferences. For example, Hann, *et al.*, observe clustering somewhat different from Westin's: "privacy guardians, information sellers, and convenience seekers."[90] In a conjoint analysis exercise with subjects from the United States and Singapore, they found that positive value is associated with certain website mechanisms to mitigate privacy concerns. At the same time, they observe that countervailing benefits, such as convenience and monetary value, significantly affect subjects' relative preferences for websites with differing privacy protections. For U.S. subjects, they estimate a low-but-positive value for "protection against errors, improper access, and secondary use of personal information."[91]

Athey, Catalini, & Tucker—in an experiment with student subjects at the Massachusetts Institute of Technology (not regarded as representative of the larger population)—found a disconnect between subjects' stated privacy preferences and their privacy-relevant behavior.[92] Students were willing to disclose personal contact information in exchange for the small reward of free pizza and were willing to do so with respect to their own personal information as well as that of their friends.

Similarly, Beresford, Kübler, & Preibusch employed a field experiment that compared subjects' choices between two stores for DVD purchases, with the stores being identical but for pricing and

---

[87] *Id.* at 1116–17.

[88] *See supra* notes 81-87, and accompanying text; *see also*, Alessandro Acquisti, Laura Brandimarte, & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015). The philosopher Judith Jarvis Thompson has said, "[p]erhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is." Judith Jarvis Thomson, *The Right to Privacy*, 5 PHILOSOPHY AND PUBLIC AFFAIRS 295, 295 (1975).

[89] WESTIN, *supra* note 83.

[90] Il-Horn Hann, Kai-Lung Hui, Sang-Yong Tom Lee, & Ivan P. L. Png, *Overcoming Information Privacy Concerns: An Information Processing Theory Approach*, 24 J. MGMT. INFO. SYS. 13 (2007).

[91] *Id.* (estimating values for U.S. subjects at $30.49-44.62).

[92] Susan Athey, Christian Catalini. & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* (NBER Working Paper 23488 (2017), http://www.nber.org/papers/w23488.

privacy policies: one priced DVDs at one euro less than the other but required the provision of more sensitive consumer data.[93] They found that "almost all buyers were willing to give up more personal information for a one Euro discount on a DVD and, even without the discount, buyers bought almost equally between two competing stores with different levels of personal information requirements."[94]

In experimental research employing both actual excerpts from privacy policies from Facebook, Google, and Yahoo, along with fictional policy excerpts, Strahilevitz & Kugler found that many subjects read the policies closely and understood them, but only about one third of subjects indicated any willingness to pay any amount of money for access to email services that would not employ content-based analysis of the users' emails to serve personalized advertising. Of those who were willing to pay anything at all, median willingness to pay was only $15 per year.[95]

Consistent with the experimental evidence cited above, many consumers may attach relatively little value to certain privacy protections, just as tens of millions voluntarily use social-media mechanisms to broadcast information others might consider sensitive.[96] For a simple example, some consumers might be "privacy fundamentalists" with regard to their financial information, while merrily posting details of their dating history on social media.

At the same time, there is evidence that privacy valuations vary across contexts; that is, whether consumers "care a lot or a little [about privacy] depends critically on context."[97] In one series of experiments, John, Acquisti, & Loewenstein found that subjects' willingness to disclose personal information was dependent on contextual cues that had little to do with objective risk factors.[98]

Tradeoffs and how consumers value them can vary across consumers, types of information, types of conduct, firms, etc. As Acquisti, Taylor, & Wagman observe:

> The value of keeping some personal information protected and the value of it being known are almost entirely context-dependent and contingent on essentially uncertain combinations of states of the world. Furthermore, privacy sensitivities and attitudes are subjective and idiosyncratic, because what constitutes sensitive information differs across individuals.[99]

---

[93] Alastair R. Beresford, *et al.*, *Unwillingness to Pay for Privacy: A Field Experiment*, 117 ECON. LETTERS 25 (2012).

[94] *Id.* at 25-6.

[95] Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEG. STUD. S69 (2016).

[96] Sarah Spiekermann, Jens Grossklags, & Bettina Berendt, *E-Privacy in Second Generation E-Commerce: Privacy Preferences Versus Actual Behavior*, in Proc. Third ACM Conf. on Electronic Commerce (eds. Michael P. Wellman & Yoav Shoham 2001); Leslie K. John, Alessandro Acquisti & George Loewenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Personal Information*, 37 J. CONSUMER RES. (2011).

[97] Alessandro Acquisti, Leslie John & George Loewenstein, *What is Privacy Worth*, 42 J. LEGAL STUD. 249, 252 (2013). *See also*, John, Acquisti, & Loewenstein, *id.* Both papers suggest that some of the variation may be independent of objective risk.

[98] John, Acquisti, & Loewenstein, *supra* note 96.

[99] Acquisti, *et al.*, *supra* note 67, at 446.

Context dependence adds a dimension of complexity to the tradeoffs implicit in privacy policy. A further complication arises when we consider the nexus (or potential disconnect) between a consumer's privacy values and those addressed—positively or negatively—in any given privacy policy, as well as between the policy and the actual risk of harm.

2. *Consumers may choose to be 'rationally ignorant' of privacy policies*

The ANPR suggests that many privacy policies are "not readable," citing research indicating that many consumers do not read privacy policies and that many who do fail to comprehend them.[100] That may suggest a problem for many consumers, if one that further disclosure research and consumer education might ameliorate. Still, there is an open question what the policy information is worth to any given consumer. Beales & Muris recognize that some consumers value privacy—and, perhaps, privacy policies—greatly, while others do not.[101] They note that, for many, a failure to digest complex privacy policies may reflect "rational ignorance":

> Consumers … maintain rational information about how much and what kind of information sharing occurs. It simply does not pay for most consumers to think and make decisions about policies on the use of their information, given that the issue is of such little practical consequence to them.[102]

Different factors may be at play for different consumers. Consider the relationships between a privacy policy as written, a privacy policy as implemented or observed by a firm, and the risk of material harm (some function of the likelihood and magnitude of harms a given consumer considers material). A consumer might attach low value to a privacy policy because the consumer attaches little value to privacy, or a consumer might attach low value to a privacy policy because she doubts the nexus between a given privacy policy and her risk of harm. Such doubt might attach to the likelihood of harm, the particular privacy values that the policy purports to address, or both.

Recall the difficulty that both private litigants and enforcement agencies may face in seeking to establish a causal link, or "proximate" cause, where there are demonstrable consumer harms. As noted above, risk-assessment experts have found it extremely difficult to assess or price risk according to variation in firm privacy policies.[103] Even privacy-sensitive consumers may reasonably question the marginal benefit they are likely to derive from any particular change in a firm's privacy policies. For many, the light shed by reading a privacy policy may not be worth the candle. Where expert agencies

---

[100] 87 FED. REG. 51275. But *see, e.g.*. Strahilevitz & Kugler, *supra* note 95.

[101] J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHICAGO L. REV. 109, 115 (2008). *See also* James C. Cooper & Joshua Wright, *The Missing Role of Economics in FTC Privacy Policy*, in CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Jules Polonetsky, Evan Selinger & Omer Tene, eds.) (2017).

[102] Beales & Muris, *id.* at 115.

[103] Research by Romanosky, *et al.,* suggests some of the challenges of risk assessment. Sasha Romanosky, *et al.*, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1 (2019) (reviewing 235 selected filing dockets, from large and small underwriters, from 2007-20017, and finding that "the first and most important firm characteristic used to compute insurance premiums was the firm's asset value (or revenue) base rate, rather than specific technology or governance controls." *Id.* at 17.)

cannot expect to fare better, it may be difficult to justify on a cost-benefit basis the value of a proposal to require one policy or another.

3. *Data security is not costless*

Diverse federal and state laws address data security, as well as privacy.[104] There are potential advantages to national data-security regulation, including some shared with the potential advantages of federal privacy regulation. These include harmonization of industry practices with a single federal standard, rather than a motley assemblage of potentially cross-cutting federal and state regulations. A single federal standard could, in theory, reduce the costs of regulatory complexity and uncertainty, and likely compliance costs as well. Those potential advantages would be diminished if additional federal regulations were merely added to the mix. The advantages of clear and uniform national rules therefore depend on federal regulations that set both "a floor and ceiling," via preemption. Full realization of that advantage would thus require further legislation, and not merely administrative initiatives, because federal data-security rules and standards are themselves diverse[105] and not susceptible to preemption by FTC rulemaking.

The National Institute of Standards and Technology defines "data security" as "the process of maintaining the confidentiality, integrity, and availability of an organization's data in a manner consistent with the organization's risk strategy."[106] On that definition, data security and data regulation are related, to the extent that data regulation and potential liability are factors in determining an organization's (or individual's) risk strategy. Data security and privacy concerns are likewise related, but distinct. Data-security measures are one way to protect at least certain privacy values, and they may be part of a firm's implementation of its privacy policies. Still, privacy concerns may arise even in the presence of rigorous data security. Data-security injuries also may be broader than privacy injuries: that is, failures or breaches of data security may lead to privacy harms, but they may also involve

---

[104] The ANPR notes diverse foreign and U.S. state-specific privacy laws, 87 FED. REG. 51276-77, along with "a number of sector-specific laws that relate to commercial surveillance practices." *Id.* at 51277 (laws and regulations enforced by the FTC under seven statutes, as well as the breach notification rule). Many data laws, such as HIPAA, and laws of general application, such as the FTC Act, reach both privacy and security matters. For a discussion of the challenges or costs of regulatory complexity in the particular domain of health care privacy, *see, e.g.*, Daniel J. Gilman & James C. Cooper, *There is a Time to Keep Silent and a Time to Speak, the Hard Part is Knowing Which Is Which: Striking the Balance between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279 (2010) (describing various federal and state regulations, id. at 301-310, and problems of complexity, id. at 345-349).

[105] *See, e.g.*, the HIPAA Security Rule, codified at 45 C.F.R. Part 160 and Subparts A and C of Part 164, "establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information." Dep't Health & Human Servs., Health Information Privacy, the Security Rule (content last reviewed Sep. 23, 2020), https://www.hhs.gov/hipaa/for-professionals/security/index.html; *see also*, Standards for Safeguarding Customer Information (Safeguards Rule), 15 U.S.C. 6801(b), 6805(b)(2); Privacy of Consumer Financial Information (Regulation P), 12 C.F.R. Part 1016 (pertaining to confidentiality and security of protected information, in addition to privacy requirements). Whereas the FTC's Safeguards Rule and the CFPB's Regulation P pertain to different entities, covered entities under the HIPPA Security Rule are typically subject to Section 5 of the FTC Act as well.

[106] NIST, *Data Security*, NAT'L CYBERSECURITY CTR. OF EXCELLENCE, https://www.nccoe.nist.gov/data-security (last visited November 11, 2022).

data that are not considered "consumer data" and harms that are not considered privacy harms. For example, data corruption or denial of service may involve valuable commercial data that is not personal data or PII, and they may not expose sensitive data to prying eyes in any case.

In some regards, data-security practices may be more amenable to regulation based on agency expertise, and less on political questions about competing policy values, even if data-security regulation would also involve questions of how to delimit and assess cognizable injuries, as well as how to structure risk strategy across organizations, categories of data, and usage. The structure of guidance provided by NIST's National Cybersecurity Center of Excellence suggests something of the complexity, as guidance can be searched by, *e.g.*, technology (13 categories) or sector (six categories). Some tradeoffs are technical (and where data security involves standard setting, whether public or private, it tends to be technology-specific) but others recall policy questions, such as tradeoffs between data security on the one hand and accessibility or portability on the other, or resolving tension between privacy and data-security goals, or between data security and accessibility or portability.

Historically, the FTC's approach to data security has resembled a negligence regime:

> The touchstone of the [FTC]'s approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.... [T]he [FTC] has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[107]

As Cooper & Kobayashi observe, that "standard comes directly from the FTC's unfairness authority under Section 5, which prohibits conduct that creates 'substantial injury to consumers' that is not outweighed by benefits to consumers or competition."[108] Based on a standard approach to the economics of accidents, efficient results can obtain under either a negligence regime or a strict-liability regime. Cooper & Kobayashi argue that, for various reasons, a strict-liability regime should be preferred, on error-cost-minimization grounds.[109]

That may be correct, but we note a prior problem in any case: efficient operation of either type of regime depends on the ability to assess damages and causality. The former takes us back to the question of how to identify and measure informational injuries; and the latter, while not necessarily intractable, can be extremely challenging in common data-security matters and simply impracticable

---

[107] Fed. Trade Comm'n, *Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf. *See also generally* Manne & Stout, *supra* note 53.

[108] 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).

[109] *Id.* at 263.

in many of them.[110] Moreover, efficient regulation of either regime is a question of both liability and remedies. Liability regimes are supposed to prompt firms to internalize the costs of their risky conduct. If damages or regulatory penalties are untethered from either actual harm or the risk of actual harm, then there is no reason to suppose that they will (or basis on which they can).

No doubt there is significant risk in aggregate. Based on data from the 2018 *Identity Theft Supplement to the National Crime Victimization Survey*, a 2021 report from the Bureau of Justice Statistics indicates "an estimated 23 million persons… reported that they had been victims of identity theft in the prior 12 months" and that "[f]inancial losses due to identity theft totaled $15.1 billion among… [those] with known losses of $1 or more (70% of all victims)."[111] That estimate is neither definitive nor comprehensive, but it is at least a crude signal of the magnitude of the problem and perhaps a lower bound for estimating consumer injury. At the same time, the survey cutoff of "known losses of $1 dollar or more" signals substantial variation that is borne out in the report, with mean losses of $800, median losses of $200, and many victims reporting no financial loss.[112]

4. Privacy and data-security values can be in conflict

A better estimate of both direct and indirect consumer injury would be extremely useful. For now, the key points are simple: aggregate data-security harms are substantial; privacy and data-security policies at both the firm and regulatory levels can conflict, prompting complex tradeoffs; and some of those tradeoffs prompt political questions about the relative values of competing policy goals.

Privacy and data security are related but distinct—and not always complementary—concepts. Data-security measures can serve to implement privacy goals by, for example, insulating sensitive personal information from prying eyes (or bots). But data-security measures can also serve to protect, for example, the integrity or accessibility of valuable data independent of the question of whether the data are sensitive or in any way personal. Moreover, privacy goals can involve measures of consumer access and control that are at odds with data-security goals. Data policy, correspondingly, sometimes entails choosing between privacy and data-security priorities. Because the ANPR raises broad questions about both privacy and data security, cost-benefit analysis required in this proceeding must account for the ways in which regulations that aim to increase user privacy can have a negative impact on security, and vice versa.

---

[110] *See* Erika Harrell, *Victims of Identity Theft: 2018*, DEP'T JUSTICE, BUREAU OF JUSTICE STATISTICS, 8 (2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf ("Most identity-theft victims did not know who the offender was or how the offender obtained their information."). While expert agencies may fair better, they too may find establishing causality to be a challenge in many individual matters and a more fundamental challenge generally. Research by Romanosky, *et al.*, suggests some of the challenges of risk assessment. Romanosky, *et al.*, *supra* note 103 at 17 (reviewing 235 selected filing dockets, from large and small underwriters, from 2007-2017, and finding that "the first and most important firm characteristic used to compute insurance premiums was the firm's asset value (or revenue) base rate, rather than specific technology or governance controls").

[111] Harrell, *id.* at 8.

[112] *Id.* at 9, table 7; *see also id.* at 3, table 1 (ID theft by type), and 6, table 4 (demographic characteristics of victims).

Both regulatory goals are concerned with preventing the undue or unauthorized use or distribution of consumer data, whether by malicious third parties or by the platforms with which users interact. Indeed, firms that work with user data often act in furtherance of both goals by securing systems, encrypting data, and maintaining internal protocols—all aimed at preventing third-party exfiltration of data as well as restricting access to user data internally to only those parties that need to work with it.

At the same time, regulatory mandates that aim to protect user privacy or to require that firms take stronger measures to prevent third parties from breaching sensitive systems can pull in opposite directions. Indeed, the European Data Protection Supervisor has acknowledged that these tensions are so important that the tradeoffs must be resolved by the legislature:

> [T]he pursuance of the objectives of cybersecurity may lead to deploying measures that interfere with the rights to data protection and privacy of individuals. This means ensuring that any potential limitation of the right to the protection of personal data and privacy must fulfil the requirements of Article 52(1) of EU Charter of Fundamental Rights, in particular being achieved by way of a legislative measure, being both necessary and proportionate, and respecting the essence of the right.[113]

For example, a regulatory requirement to treat user browsing data as "covered data," as has been advanced in the American Data Privacy and Prevention Act,[114] can make it difficult to rely on user logs to detect unusual patterns of behavior that may suggest potential hacking attempts. Similarly, creating expansive privacy rights, such as requiring firms to give users a right to deletion or a right to access, can expose additional vectors whereby malicious third parties can obtain or otherwise interfere with a user's data. Mandates that prevent firms from securely storing long-term backups create problems when systems are subject to ransomware attacks.[115]

This is not unilaterally true for every privacy or security regulation. The nature and magnitude of any security vulnerabilities created by privacy rules are difficult to know *ex ante*, or as a general matter, but this problem is sufficiently prevalent that the Commission needs to keep it in mind when designing any rules. Any "commercial surveillance" rule aimed at increasing protections for user privacy raises the specter of both mixed and unintended effects, including, *inter alia*, reduced data security associated with enhanced user access or control; more costly or less-effective monitoring of consumer usage for account security and integrity; reduced accuracy of identification and authentication; and other vulnerabilities that might be exploited by third parties.

---

[113] European Data Protection Supervisor, Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, at 11 (2021), *available at* https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.

[114] H.R. 8152, American Data Privacy and Prevention Act, 117th Cong. (2021-22).

[115] Being able to restore data from a secure backup is one of the chief means of responding to a system compromised by a ransomware attack. *See, e.g.*, Amrit Singh, *Guide to How to Recover and Prevent a Ransomware Attack*, BACKBLAZE.COM (Jul. 29, 2022), https://www.backblaze.com/blog/complete-guide-ransomware.

a. The EU experience with GDPR illustrates potential conflicts between privacy and data security

One of the clearest examples of this tension can be found in the European experience with GDPR. According to Layton & Elaluf-Calderwood, implementation of the GDPR has "increased cyber risk notably with [the domain-name system] and identity theft."[116] Among the ways that GDPR poses risks to cybersecurity is the tendency of European data-protection authorities to push in the direction of data localization. On such an interpretation, personally identifiable information (interpreted so broadly as to include information about IP addresses) cannot be shared outside of the European Union without safeguards. Swire & Kennedy-Mayo, cataloguing the negative effects of data localization,[117] concluded that "net benefits of localization on breaches seem subject to doubt, because there is no particular reason to believe that drawing lines based on national borders is the optimal approach to minimizing the likelihood and magnitude of harm from a breach."[118] The authors also discussed in detail the ways in which data localization created obstacles for integrated cybersecurity management.[119]

"Rights" to access and data portability provide data subjects, upon request, with information on the data regarding them that is being processed by a firm or data processor, along with certain means to transfer that data. The first obvious security (and privacy) concern that those rights create is that it may be possible to impersonate another person and then to request their data (*e.g.*, from a social-media service).[120] Hence, we might expect data processors to be cautious and only provide the information if sufficient proof of identity is presented to them. The risks of impersonation can be mitigated, but they cannot be eliminated. This is especially true if, for example, attackers are willing to use fake ID documents or if they have already gained control of the victim's email account. Moreover, mitigation measures like requesting ID documents are likely to create new risks. As Boniface, *et al.*, note:

> First, a security incident can occur on the data controller's side and the copy of the data subject's ID document can be leaked to attackers. Second, the data controller (or the attacker from the previous case) can *impersonate* the data subject to other data controllers by using her ID document to exercise the subject access requests on her behalf. Moreover, with the data subject's ID document it is possible to impersonate her at any point in the future (until the ID document expires).[121]

---

[116] Roslyn Layton & Silvia Elaluf-Calderwood, *A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices*, IEEE (2019), *available at* https://ieeexplore.ieee.org/abstract/document/8962288.

[117] Peter Swire & DeBrae Kennedy-Mayo, *The Effects of Data Localization on Cybersecurity*, Georgia Tech Scheller College of Business Research Paper No. 4030905 (2022), *available at* https://ssrn.com/abstract=4030905.

[118] *Id.* at 16

[119] *Id.* at Annex I.

[120] Coline Boniface, *et al.*, *Security Analysis of Subject Access Request Procedures*, in PRIVACY TECHNOLOGIES & POL'Y. APF 2019. (Maurizio Naldi, *et al.* eds., 2019). *See also* Peter Swire & DeBrae Kennedy-Mayo, *supra* note 117.

[121] *Id.*

The right to be forgotten (the right to erasure of personal data or, at least, the entitlement to certain impediments to searches for that data) created tensions with one of the key aspects of modern data security: data backups.[122] Protecting backups from modification (including from being overwritten) is an important element of prevention or mitigation of attacks that compromise user data in a production environment. For example, this can be ensured by using a write-once medium. Requiring data processors to technically enable erasure of individual personal data in backups opens a potential vector of attack, as it means enabling a modification of a backup. Some national data-protection authorities have recognized that there may be technical reasons against this. For example, the UK Information Commissioner's Office ("ICO") stated that it may be justified to keep personal data until the backup "is replaced with an established schedule."[123] But even then, according to the ICO, the personal data in question must be put "beyond use," which may cause significant problems in cases where there is a need for a rapid system-restore procedure—*e.g.*, following a ransomware attack.

5. By congressional design, the FTC's privacy authority, expertise, experience, and resources are substantial but limited

a. Congress has partitioned and limited federal privacy and data-security-enforcement responsibilities.

As noted in the ANPR, Congress has expressly charged the FTC with certain privacy and data-security regulation and Congress continues to consider additional federal privacy laws. The Commission's experience and expertise in the enforcement of Section 5 and special data statutes is considerable, but it is also limited. Not incidentally, in every statute in which Congress expressly sets forth privacy or data-security provisions, Congress recognizes tradeoffs between privacy and other important values related the flow of information. For example, in the Fair Credit Reporting Act,[124] Congress recognized the need for both the "accuracy and fairness of credit reporting," noting that "[i]naccurate credit reports directly impair the efficiency of the banking system," and that "unfair credit reporting methods undermine public confidence."[125] Specific provisions recognize numerous policy goals, including but not limited to privacy. For example, consumer reporting agencies may furnish reports as requested by the individual subject of a report, but also in response to court orders or in response to a request from a person the reporting agency "has reason to believe" will use the information for, *inter alia*, evaluating various credit transactions and accounts, insurance underwriting, and employment purposes.[126] The FCRA also authorizes reporting for national-security

---

[122] Eugenia Politou, *et al.*, *Backups and the Right to Be Forgotten in the GDPR: An Uneasy Relationship*, 34 COMPUTER L. SEC. R. 34. 6 (2018).

[123] UK Information Commission's Office, *Right to Erasure*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#ib5 (*last visited* Nov. 3, 2022).

[124] 15 U.S.C. § 1681 et seq.

[125] *Id.* at § 1681(a)(1).

[126] *Id.* at § 1681b(a)(1)-(3)

purposes,[127] law-enforcement purposes,[128] and, in particular, to state or local child-support enforcement agencies.[129]

The full title of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[130]—grounds for significant privacy and data-security regulation in the health-care sector—describes it as an act to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[131] Privacy provisions were not prominent, although Section 264 of HIPAA did charge HHS to report to Congress on "recommendations on standards with respect to the privacy of individually identifiable health information," within 12 months of the statute's enactment.[132] The statute also provides that HHS should undertake rulemaking with respect to such standards if Congress did not enact pertinent statutory provisions within 36 months of HIPAA's enactment.[133] Recent provisions of the 21st Century Cures Act similarly recognizes privacy interests, while also mandating interoperability and prohibiting "information blocking" regulation and enforcement by HHS;[134] in essence, imposing positive duties to deal for certain health information and health-information technology.[135]

Congress has also charged specific authorities with enforcement responsibility for these statutes. For example, while HHS is HIPAA's primary enforcer,[136] it refers certain matters to the DOJ for criminal investigations, and state attorneys general also may bring enforcement actions in *parens patriae*.[137] For the FCRA, as amended, enforcement authority is now shared. The FTC, importantly, retains some of its initial enforcement authority.[138] Equally important, however, is that Congress took deliberate steps to augment and partition that enforcement authority with amendments to the FCRA, providing for, *e.g.*, actions brought by state attorneys general in 1987,[139] and assigning considerable

---

[127] Id. at § 1681(u).

[128] Id. at § 1681(f).

[129] *Id.* at § 1681b(a)(4).

[130] Pub. L. 104-191 (Aug. 21, 1996).

[131] *Id.*

[132] *Id.* at Sec. 264.

[133] *Id.*

[134] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Criteria, 84 FED. REG. 7424, 7424 (proposed Mar. 4, 2019) (to be codified at 45 C.F.R. Parts 170 and 171).

[135] Fed. Trade Comm'n., FTC Staff Comment Before Dep't Health & Human Servs. Regarding the 21st Century Cures Act: Interoperability and Information Blocking, and the ONC Health IT Certification Program (2019), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-department-health-human-services-regarding-21st-century-cures-act-interoperability/v190002_hhs_onc_info_blocking_staff_comment_5-30-19.pdf.

[136] 14 U.S.C. § 1320d-5(a)(1).

[137] *Id.* at § 1320d-5(d).

[138] 15 U.S.C. § 1681s(a)(1)

[139] 15 U.S.C. § 1681s(c).

regulatory authority to the Consumer Financial Protection Board as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[140]

There is, as well, the question of resource allocation that may come with an express statutory charge. We cannot gainsay the importance of the FTC's privacy and data-security enforcement work under Section 5 of the FTC Act. At the same time, we cannot help but notice a misfit between congressionally allocated resources and the obligations entailed by data regulations of the scope contemplated in the ANPR. By way of contrast, we note that, since the compliance date of the HIPAA privacy rule, the HHS Office of Civil Rights ("OCR") has investigated and resolved nearly 30,000 cases involving HIPAA-covered entities and their business associates; for appropriate cases of knowing disclosure of or obtaining protected health information, OCR has referred more than 1,500 cases to DOJ for criminal prosecution.[141]

b. Regulation of the ANPR's scope and likely economic consequence implicates the major questions doctrine

In his dissent from the issuance of this ANPR, Commissioner Phillips noted the massive scale and complexity of the undertaking it initiates:

> Legislating comprehensive national rules for consumer data privacy and security is a complicated undertaking. Any law our nation adopts will have vast economic significance. It will impact many thousands of companies, millions of citizens, and billions upon billions of dollars in commerce. It will involve real trade-offs between, for example, innovation, jobs, and economic growth on the one hand and protection from privacy harms on the other. (It will also require some level of social consensus about which harms the law can and should address.) Like most regulations, comprehensive rules for data privacy and security will likely displace some amount of competition. Reducing the ability of companies to use data about consumers, which today facilitates the provision of free services, may result in higher prices—an effect that policymakers would be remiss not to consider in our current inflationary environment.[142]

These considerations all militate in favor of regulatory restraint by the FTC as a matter of policy. They also require restraint, and an emphasis on established jurisdiction, given the Supreme Court's recent "major questions" jurisprudence.[143] As noted in the statements of several commissioners,[144] *West Virginia v. EPA*[145] clarifies the constitutional limits on an agency's authority to extend the reach

---

[140] Pub. L. 111-203, 111th Cong. (Jul. 21, 2010). Title X of the Act, § 1001 et seq., establishes the CFPB, with FCRA enforcement authority codified at 15 U.S.C. § 1681s(b)(1)(H).

[141] Dep't Health & Human Servs., Health Information Privacy, Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (*last visited* Sep. 14, 2022).

[142] ANPR, *supra* note 1, at 51293 (Dissenting Statement of Comm'r Noah Phillips).

[143] *See* W. Virginia v. Env't Prot. Agency, 142 S. Ct. 2587, 2595 (2022).

[144] *Compare* 87 FED. REG. 51295 (Statement of Commissioner Phillips) and id. at 51298-99 (Statement of Commissioner Wilson) *with* id. at 51288-90 (Statement of Commissioner Slaughter).

[145] W. Virginia v. Env't Prot. Agency, 142 S. Ct. 2587.

of its jurisdiction via regulation. In brief, the broader the economic and political sweep of data regulations the Commission might propose, the more likely it is that such regulations exceed the FTC's authority.

The "major questions doctrine" is framed as a matter of statutory interpretation, but one where the means or manner of construction "must be 'shaped, at least in some measure, by the nature of the question presented.'"[146] In "extraordinary cases, the 'history and breadth' of an agency's claim to authority, and its 'economic and political significance'" provide "a reason to hesitate before concluding that Congress' meant to confer such authority."[147] Such cases require "more than a merely plausible textual basis for the agency action"; they require "clear congressional authorization" for the authority claimed by an agency.[148]

If the major questions doctrine is implicated, the burden is on the agency to establish the specific grant of authority that is claimed: "Even if Congress has delegated an agency general rulemaking or adjudicatory power, judges presume that Congress does not delegate its authority to settle or amend major social and economic policy decisions."[149] Moreover, the Court was clear that a colorable claim of statutory implementation is inadequate to establish the authority to issue sweeping regulations with major economic and political implications. Hence, in *National Federation of Independent Business v. OSHA*, the Court determined it "very unlikely" that Congress had delegated the claimed authority to the agency, notwithstanding that "[a]ll of… [the] regulatory assertions had a colorable textual basis."[150]

That requirement is shaped not simply by general principles of statutory construction, but by "separation of powers principles."[151] In that respect, as Justice Gorsuch noted in his concurring opinion, the questions raised in *West Virginia v. EPA* also sound in non-delegation concerns about the limits of the congressional power to delegate its legislative authority, independent of the specificity with which it may attempt to do so.[152]

As we have discussed, the ANPR does not propose or even sketch a possible "commercial surveillance and data security" regulation. For that reason, among others, the question whether such a rule runs afoul of the major questions doctrine depends as much on the particulars of a hypothetical proposal as it does on judicial application of the doctrine. Still, we cannot help but notice—and the Commission should not fail to notice—that the full scope of the inquiry suggested in the ANPR exceeds that which implicated the major questions doctrine in *West Virginia v. EPA*. General data

---

[146] *Id.* at 2608.

[147] *Id.* at 2595.

[148] *Id.*

[149] *See id.* at 2613 (*citing* WILLIAM ESKRIDGE, INTERPRETING LAW: A PRIMER ON HOW TO READ STATUTES AND THE CONSTITUTION 288 (2016)).

[150] *Id.* at 2608-09.

[151] *Id.*

[152] *Id.* at 2616 (Gorsuch, J. concurring).

regulations, including but not limited to privacy and data-security regulations, would have tremendous economic and political consequences. All of the observations made by the Commission in favor of its jurisdiction cut both ways: the FTC's regulatory jurisdiction is wide-ranging, but it is subject to substantial constraints, both procedural and substantive;[153] Congress has granted the FTC enforcement authority with regard to certain privacy and data-security matters, but it has assigned such authority over some matters to several federal agencies and not exclusively to the FTC.[154]

Commissioner Slaughter suggests that "the questions we ask in the ANPR and the rules we are empowered to issue may be consequential, but they do not implicate the 'major questions doctrine.'"[155] Surely, Commissioner Slaughter is right that questions posed in an ANPR do not, in and of themselves, raise major questions concerns. Congress assigned wide-ranging research and reporting authority to the FTC under Section 6, with an express charge to report economic and policy findings to Congress, among others.[156] Such research and reporting does not usurp congressional legislative authority; it serves that authority, just as it serves Commission enforcement within the bounds of Section 5. As we have argued, and as implied by the breadth of the questions posed in the ANPR, there is much economic and policy research that needs to be done if broad data laws and regulations are to reflect a serious consideration of costs and benefits. But Commissioner Slaughter's suggestion that major questions are not *implicated* by the questions posed in this ANPR is far too easy: it is precisely because the issues raised by the ANPR—and by the scope of potential intervention—are consequential that the major questions doctrine is most surely implicated.

III. Data Regulations Can Have Complex, and Sometimes Negative, Effects on Competition

As acknowledged in the ANPR, FTC rulemaking under the Commission's Section 18 unfairness authority requires, among other things, that regulations address substantial consumer injuries "not reasonably avoidable by consumers themselves *and not outweighed by countervailing benefits to consumers or to competition*."[157] In that regard, the ANPR appropriately raises several questions about the potential impact of "any given new trade regulation rule on data security or commercial surveillance" on competition.[158] In an orthogonal footnote, the Commission also "invites comment on the ways in which existing and emergent commercial surveillance practices harm competition and on any new

[153] 87 FED. REG. 51277-79.

[154] *Id.* at 51278; *supra* text accompanying notes 136-140.

[155] 87 FED. REG. 51290 (Statement of Commissioner Rebecca Kelly Slaughter).

[156] 15 U.S.C. § 46(a)-(b).

[157] 87 FED. REG. 51278 (emphasis added).

[158] 87 FED. REG. 51282-83 (ANPR questions 27, 40, and 52).

trade regulation rules that would address such practices," and queries whether such a regulation might be adopted without the strictures of Section 18.[159]

Unfortunately, the ANPR has not specified or even provisionally sketched potential "commercial surveillance and data security" regulations; thus, the competitive effects of an unspecified rule are hard to estimate. But as we detail below, the developing body of literature on the impact of data regulations on competition and innovation suggest the need for both substantial research and regulatory humility. As we also explain below, and more thoroughly in comments submitted separately to the record of this proceeding, the Commission has no grounds on which to consider adopting privacy or data-security regulations under its UMC authority.

The statutory requirements of Sections 5 and 18 roughly mirror some of the more general grounds on which one might consider regulation: observation of substantial net consumer harms due to market failure in some domain of commercial conduct. Good policy also requires an effective and efficient regulatory solution; that is, the ability of regulators to do more good than harm, such that regulatory benefits are not outweighed by countervailing harms to consumers or to competition. The likely competitive effects of any given rule commonly receive far too little consideration in regulatory design. But such considerations are basic to coherent intervention by the FTC, an agency charged with dual competition and consumer-protection missions that are supposed to be mutually reinforcing. Regulatory benefits might comprise, among other things, a direct increase in consumer welfare (via the diminution of harm or otherwise) or improvements in competition, such that the market might better provide consumer benefits. Harms, correspondingly, might include direct harms, harms to competition (which are likely to harm consumer welfare), and harm to innovation or dynamic competition (which also are likely to harm consumer welfare).

Issues at the nexus of privacy, data security, and competition have been considered in prior Commission proceedings, including numerous days of sessions in the FTC's Hearings on Competition and Consumer Protection in the 21st Century, and in written comments submitted to the record of those hearings. To the best of our knowledge, the Commission has not yet reported findings from these hearings. As we noted in the Executive Summary of these comments, ICLE provided extensive input on data regulation and competition to the hearings record.[160] We are re-submitting those prior written comments separately, to this proceeding, for the Commission's convenience.

---

[159] *Id.* at 51276 at n. 47. ANPR question 66 raises the competition question with regard to "algorithmic discrimination" *Id.* at 51284. While the ANPR raises numerous questions about harms associated with commercial-data practices and several about the potential impact of regulations on competition, the 95 enumerated compound questions in the ANPR do not include any that ask directly about consumers' abilities to avoid harms .Several questions inquire about the effectiveness of, *e.g.*, consent, or of opt-in requirements in particular, 87 FED. REG. 51284, none asks more generally about the ways in which or degrees to which consumers may reasonably avoid informational injury.

[160] *See, e.g.*, Dirk Auer, *et al.*, *Privacy, Antitrust, and the Economic Approach to the Regulation of Consumer Data (FTC Hearings, ICLE Comment 4),* Comments of the Int'l Ctr. for Law & Econ. Submitted to the Fed. Trade Comm'n Hearings on Competition and Consumer Protection in the 21st Century, Topic 3: The Regulation of Consumer Data (2019), https://laweconcenter.org/resource/icle-comments-the-regulation-of-consumer-data; *See also* FTC Hearings on Comp. and

Below, we consider the literature regarding the demonstrated and likely effects of data regulation on competition. In addition, we briefly review some of the issues regarding antitrust consideration of privacy that were discussed at length in our 21st Century Hearings submission.

A. Many of the Documented Effects of Privacy Regulations on Competition are Negative

It is impossible to fully predict the effect of something so amorphous as "any given potential trade regulation rule."[161] Still, some general observations should help to guide the Commission's inquiry. As a 2020 note by the United States to the Organisation for Economic Co-operation and Development ("OECD") observed, "[s]ome data rights and obligations may enhance competition, for instance, by reducing information asymmetries or by deterring exclusionary conduct."[162] At the same time, however, the U.S. government sounded an important note of caution:

> Other rights and obligations may impair competition, for instance, by entrenching market power. For example, Campbell, Goldfarb, and Tucker use a microeconomic model to argue that, due to economies of scale in data collection and utilization, certain privacy regulations, though imposing costs on all firms, may have a particularly adverse effect on smaller and new firms, especially in cases where firms offer zero-priced consumer services.[163]

At the broadest level, any regulatory regime imposing substantial fixed costs will have some competitive effects.[164] As Catherine Tucker & Alex Marthews explain in a Brookings Economics Report:

> From an economics perspective, when modeling the effects of privacy regulation on the ability of firms to compete, one starting point is the observation that in theory, any regulation that imposes any fixed costs on firms will have an anti-competitive effect… . The concern is that if compliance has a fixed cost, then that fixed cost will be more heavily

---

Consumer Protection in the 21st Century, Data Security Hearings, Testimony of Geoffrey Manne, Int. Ctr. for Law & Econ. (Dec. 12, 2018), *transcript at* https://www.ftc.gov/system/files/documents/public_events/1418261/ftc_hearings_session_9_transcript_day_2_12-12-18_0.pdf.

[161] 87 FED. REG. 51281. Elsewhere, the ANPR asks about, *e.g.*, the effects of "any given new trade regulation rule." *Id.* at 51282.

[162] OECD, Directorate for Fin. and Enterprise Affs. Comp. Comm., Consumer Data Rights and Competition—Note by the United States, 4 (Jun. 12, 2020), https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/oecd-consumer_data_rights_us_submission.pdf (presented to OECD by FTC Commissioner Noah Phillips) (internal citations omitted); *see also, e.g.*, Timothy J. Muris, *The Interface of Competition and Consumer Protection*, FORDHAM CORP. LAW INST. TWENTY-NINTH ANNUAL CONF. ON INT. ANTITRUST LAW & POL'Y (Oct. 31, 2002) (prepared remarks of the FTC Chairman).

[163] Note by the United States at 4 (*citing* James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47 (2015)).

[164] *See, e.g.*, Caleb S. Fuller, *The Perils of Privacy Regulation*, 30 REV. AUSTRIAN ECON. 30193 (2017).

> felt by a smaller firm with smaller revenues, putting smaller firms at a cost disadvantage relative to larger firms, or at least only weakly increasing in firm size.[165]

Similarly, Campbell, Goldfarb, & Tucker demonstrate that privacy regimes that include a consent requirement can exacerbate the competitive skew in favor of incumbents.[166] In brief, the likelihood of consumer consent will vary according to, among other factors, (a) the longevity of a consumer's relationship with a given firm and (b) the scope of benefits consumers expect to receive from the firm (and, hence, from the grant of consent). These will tend to favor established firms (incumbents) and firms offering a broader array of products or services, even where a smaller "niche" firm offers a higher quality product or service.[167] They show that "privacy regulation can preclude profitable entry by the specialist firm," and that the impact of these types of regulations are "strongest in industries with little price flexibility," which may be especially important for ad-supported or other zero-price Internet products.[168]

In addition, the Commission should consider that even good-faith and productive contributions of incumbents to the rulemaking process, standard setting, and related activities may further tilt the field to the extent that costly compliance practices are not merely fixed costs but, for at least some incumbents and to some extent, both fixed and sunk.

For example, Marthews & Tucker suggest an example of the potential competitive impact of the Fair Credit Reporting Act ("FCRA"), an early federal foray into express privacy regulation:

> In its introspective into its experience with the FCRA, the FTC strikingly did not examine the competitive effects of the Act through its 40-year experience in its enforcement.... However, it is notable that the four large credit reporting agencies (Equifax, Experian, Innovis and TransUnion) have seen little competitive entry over the past decades, despite huge shifts in the nature of data and data collection due to the digital revolution, and the incumbent firms experiencing significant scandals relating to consumer privacy. We speculate that a potential explanation is that it is hard for a smaller entrant in this space to achieve even the levels of consent and compliance practiced by the incumbent credit reporting agencies.[169]

The magnitude of these competitive effects may vary substantially according to the scope of the regulation in question and its other effects. Still, they are likely competitive distortions that may be substantial and should be accounted for in any regulatory scheme. While pertinent empirical findings are by no means comprehensive, there is a growing body of applied literature on the potential

---

[165] Alex Marthews & Catherine Tucker, *Privacy Policy and Competition*, ECON. STUD. AT BROOKINGS 8 (2019), https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf.

[166] Campbell, Goldfarb & Tucker, *Privacy Regulation and Market Structure*, *supra* note 163.

[167] *Id.* at 48.

[168] *Id.*

[169] Marthews & Tucker, *supra* note 165, at 12; *see also* Fed. Trade Comm'n, FORTY YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT (2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

costs—including costs to competition and innovation—attending certain privacy and data-security regulations.

Kim & Wagman, for example, examined the impact of local opt-in and opt-out default requirements that determine whether mortgage lenders can share information about consumers applying for loans.[170] Using variation in the adoption of local financial-privacy ordinances in five California Bay Area counties, they observe that more stringent restrictions on sharing consumer financial information[171] may reduce price competition. They suggest this may be due to sellers' inability to offset potential downstream costs from loan defaults with revenues from monetizing information obtained in the application process, reducing lenders' incentives to screen applications from consumers; that, in turn, can contribute to higher rates of loan defaults.

In the health-care sector, Miller & Tucker have examined the effects of privacy protections and concerns on the flow of health-care information.[172] They found that large hospital systems are much more likely to share data internally than with third-party providers, whereas smaller providers were more likely to share data with other providers. Considering those results and prior studies, Marthews & Tucker suggest that "privacy protection in healthcare may inadvertently encourage larger hospital systems to create data silos, which exclude smaller providers."[173] In response to concerns about such data silos, Congress adopted certain mandatory "information blocking provisions"—affirmative duties to deal in information and certain health information technology—in the 21st Century Cures Act. That law charged HHS with implementation and enforcement,[174] although it is premature to evaluate either the effectiveness or efficiency of that response.[175]

---

[170] Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, 46 RAND J. Econ. 1 (2015).

[171] Specifically, in 2002, three out of five counties in the San Francisco-Oakland-Fremont, California Metropolitan Statistical Area adopted local ordinances that were more protective than previous practices, in that the new ordinances required financial institutions to seek written waivers from consumers before sharing information about those consumers with either affiliates or non-affiliates.

[172] Amalia R. Miller & Catherine Tucker, *Health Information Exchange, System Size and Information Silos*, 22 J. HEALTH ECON. 28 (2014).

[173] Marthews & Tucker at 13 (citing Miller & Tucker, note 11, *supra*, and Amalia R. Miller and Catherine Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records*, 55 MGMT. SCI. 1077 (2009)).

[174] *See, e.g.*, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Criteria, 84 FED. REG. 7424, 7424 (proposed Mar. 4, 2019) (to be codified at 45 C.F.R. Parts 170 and 171).

[175] As the Commission will recall, Congress instructed HHS to consult with FTC on competition aspects of the rulemaking, with FTC providing both informal and formal input. FTC Staff Comments on the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Rule (2020), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-letter-department-health-human-services-concerning-21st-century-cures-act-interoperability/v190002hhsinfoblockingletter.pdf;
FTC Staff Comments on the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule (2019), https://www.ftc.gov/legal-library/browse/advocacy-filings/ftc-staff-comment-department-health-human-services-regarding-21st-century-cures-act-interoperability.

In another study, Adjerid, Acquisti, & Adler-Milstein found somewhat mixed results.[176] Comparing the formation of Health Information Exchanges ("HIEs") in states that limit information disclosure (independent of the HIPAA floor) with states that do not, they observed that, in their sample, certain relatively strong privacy policies tended to suppress HIE adoption. But they also found that the combination of adoption subsidies and some stronger privacy protections was associated with greater HIE adoption than subsidies, stronger privacy protections, or weaker privacy protections alone.

Studies of the effects of data-breach laws are incomplete, and somewhat mixed, but research by Romanosky, Telang, & Acquisti suggests some positive effects on average associated with data-breach disclosure laws, which may reduce the incidence of identity theft, although it did not find that stronger breach laws were more effective than weaker ones.[177] Subsequent research by Sullivan & Maniff found that certain breach-notification provisions were associated with reduced identity theft while other provisions were associated with increased identity theft.[178]

Several studies examine the impact of broader data regulations—GDPR in particular—on the digital economy. For example, Goldfarb & Tucker studied the impact of the EU's Privacy and Electronic Communications Directive[179]—a predecessor to GDPR—on the performance of advertising in the countries that enacted it, relative to ad performance in Europe prior to the directive and to performance in nations without the directive's restrictions.[180] They found that, on average, ads became less effective relative to their performance in nations without the directive's restrictions. Moreover, they found the effect was greater for websites with general content, such as news sites, and for ads with a smaller presence on those websites.

Jia, Jin, & Wagman studied some of the effects of GDPR, analyzing data from two databases that track global venture investments.[181] Such investments are key inputs into both innovation and entry. They found evidence suggesting dramatic overall drops in investments in newer EU technology ventures after GDPR, observing especially strong impacts on consumer-facing ventures in early stages of development. This was, to be clear, a study of the early impact of GDPR, with further investigation warranted. Still, the magnitude of their early findings suggests the potential for substantial effects, at least for certain data rights.

---

[176] Idris Adjerid, Alessandro Acquisti, & Julia Adler-Milstein, *Impact of Health Disclosure Laws on Health Information Exchanges*, 65 MGT. SCI. 1949 (2019).

[177] Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGT. 256 (2011).

[178] Richard J. Sullivan and Jesse Leigh Maniff, *Data Breach Notification Laws*, FED. RES. BANK OF KANSAS CITY (2016), https://www.kansascityfed.org/documents/336/2016-Data%20Breach%20Notification%20Laws.pdf.

[179] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[180] Goldfarb & Catherine E. Tucker, *Privacy Regulation*, *supra* note 30, at 57.

[181] Jian Jia, Ginger Zhe Jin, & Liad Wagman, *The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment*, 40 Marketing Sci. 661 (2021).

Adjerid & de Matos studied a series of field experiments launched by a large telecom provider after GDPR.[182] The field experiments had been designed to foster user consent, as required under GDPR, and the study indicated that the field tests were highly successful. As a result, the telecom provider was able to process more personal data after GDPR than it was before. To the extent this finding can be generalized, it may suggest that large well-resourced firms are better able to minimize the impact of GDPR (and similar regulations) on consumer access, in addition to the general incumbency advantages described by Campbell, *et al.*

A working paper by Goldberg, Johnson, & Shriver examines GDPR's impact on firms' ability to measure the spending and site visits from EU consumers, finding declines in spending and visits of as much as 7% in the pertinent part of 2018, relative to 2017.[183] Moreover, the study indicates that, for e-commerce sites, the effects on orders were roughly four times greater for small firms than they were for larger firms.

Effects on product quality, price, and information availability have also been observed:

> Perhaps the most well-known and visible effects of the constraints imposed by GDPR on US firms are the effects on the news media. Many European users have reported instances of US newspapers not displaying content within EU borders.... this includes well-known newspapers with long histories and nationwide reach, such as the Chicago Tribune and the LA Times. ... [In addition] USA Today developed a slimline version of their website with no ads, which showed only a few stories to visitors from the EU. Newspapers such as the Washington Post charged a higher price to EU residents and provided a non-tracking version of the newspaper.[184]

There is also evidence that GDPR depressed investment in start-up app development, suppressed entry, and induced exit by a large number of small app developers. Janßen, *et al.*, surveyed 4.1 million apps on the Google Play store between 2016 and 2019 and observed that "GDPR sharply curtailed the number of available apps."[185] In particular. "GDPR precipitated the exit of over a third of available apps; and following its enactment, the rate of new entry fell by 47.2 percent, in effect creating a lost generation of apps."[186]

---

[182] Idris Adjerid & Miguel Godinho de Matos, *Consumer Behavior and Firm Targeting after GDPR: The Case of a Telecom Provider in Europe*, 68 MGMT. SCI. 3330 (2019).

[183] Samuel Goldberg, Garrett Johnson, & Scott Shriver, *Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes* (2022), *available at* https://ssrn.com/abstract=3421731.

[184] Marthews & Tucker, *supra* note 165, at 20.

[185] Janßen, *et al.*, *GDPR and the Lost Generation of Innovative Apps*, NBER Working Paper Series (2022) at 2, *available at* https://www.nber.org/system/files/working_papers/w30028/w30028.pdf.

[186] *Id.*

1. More work needs to be done to understand the interplay of data regulation and competition

There is no simple answer to the ANPR's questions about the likely impact of new data regulations and competition.[187] Privacy and data-security regulations inevitably involve complex tradeoffs among policy goals and across consumers and firms. Pertinent theoretical and empirical work is informative but incomplete. It does not completely describe the impact of any extant privacy or data-security regime; and it cannot predict the likely impact of some unspecified FTC regulation on consumer welfare or on competition.

The literature does, however, suggest caution, especially in considering general data regulations. It provides a positive answer to the ANPR's question regarding whether new rules might serve to reinforce the market power of an established incumbent, even if the magnitude of that effect might vary according to many factors, including the particulars of a given rule, as written, and as enforced.[188] It indicates real and substantial costs of certain regulations, and likely costs to competition and consumers generally—not just to regulated firms—for future regulation. Studies of GDPR in particular suggest special caution with regard to general or cross-sector data regulations. Many in Europe had proposed that GDPR would be "an enabler of competition."[189] For example, at an FTC hearing on Big Data, Privacy, and Competition, Rainer Wessely of the European Union's delegation to the United States reviewed several possible competitive advantages to the European approach and GDPR, concluding that, "eventually the GDPR should stimulate innovation and competition."[190] We are unaware of credible systematic studies demonstrating that GDPR has produced countervailing benefits for competition or consumers, such as reduced consumer harm, lower risk of identity theft, or enhanced entry or innovation. Early suggestions from Europe of competitive benefits[191] may be substantiated someday, to some extent, and in some regard, but thus far, they run contrary to the available evidence.

More generally, there is sparse literature showing marginal benefits flowing from the adoption of new privacy or data-security regulations. That is not to say that there have not been or cannot be such benefits. Rather, it is to illustrate a substantial research task that should be undertaken before the Commission considers any broad "commercial surveillance" rulemaking. We believe that the

---

[187] 87 FED. REG. 51282.

[188] *Id.*

[189] Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century, Big Data, Privacy, and Competition (Nov. 6-8, 2018) at 269 (testimony of Renato Nazzini), https://www.ftc.gov/system/files/documents/public_events/1418633/ftc_hearings_session_6_transcript_day_2_11-7-18_1.pdf.

[190] *Id.* at 290 (testimony of Rainer Wessely).

[191] *See id.* (testimony of Rainer Wessely); *cf.* Marco Botta & Klaus Wiedemann, *The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*, 64 ANTITRUST BULLETIN 428 (2019) (recognizing different goals of competition and consumer-protection law, but also maintaining that "[a] number of provisions contained in the GDPR aim at tackling a number of market failures in digital markets, such as those requiring the data subject's 'informed' consent. In addition, by sanctioning misleading and aggressive commercial practices, consumer law also safeguards the final consumer's 'informed' choice.").

FTC is well-positioned to undertake some of the requisite research and to foster more of it, given the Agency's experience with both competition and consumer-protection matters, and its considerable human capital for research in both industrial organization and consumer-protection economics. Without more, the Commission will be in no position to answer its own question about the potential impact of "any given new trade regulation rule on data security or commercial surveillance"[192] on competition, or on consumer welfare.

B. Competition and Privacy

In a footnote, the Commission notes that several petitions have suggested the possibility of privacy rulemaking under the FTC's competition authority—that is, under the Section 5 prohibition of unfair methods of competition ("UMC").[193] Accordingly, the Commission inquires about "the ways in which existing and emergent commercial surveillance practices harm competition and on any new trade regulation rules that would address such practices."[194] The concerns voiced in the petitions that the Commission cites are part of a broader family of issues regarding the treatment of personal data as a competition matter.[195] ICLE discussed many of those issues in extensive comments submitted to the record of the FTC's Hearings on Competition and Consumer Protection in the 21st Century.[196]

In short, further inquiry into various issues to do with competition and consumer data may be needed, but the Commission should not consider the adoption of privacy regulations under its UMC authority at this time. The Commission's experience in data matters does not support it and, leaving aside speculative proposals, neither does the larger body of technical and economic literature.

For decades, the Commission has brought diverse privacy and data-security cases under its UDAP authority. For more than 100 years, the Commission has enforced the federal antitrust laws—including the FTC Act and, by incorporation, the Sherman and Clayton Acts—to protect the public against anticompetitive mergers and anticompetitive conduct. In all that time, the Commission has never brought, much less won, a UMC privacy case. And where the Commission has considered a privacy

---

[192] 87 FED. REG. 51282.

[193] 87 FED. REG. 51276, at n. 47. The Commission suggests that "[s]uch rules could arise from the Commission's authority to protect against unfair methods of competition, so they may be proposed directly without first being subject of an advance notice of proposed rulemaking." But that seems a red herring. The fundamental barriers to adopting a competition rule regarding privacy are not the requirement of an ANPR or other special procedures implicated by Section 18; rather, they are substantive.

[194] *Id.*

[195] *See generally, e.g.*, Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century, Hearing 6: Privacy, Big Data and Competition (Nov. 6-8, 2018), https://www.ftc.gov/enforcement-policy/hearings-competition-consumer-protection.

[196] Auer, *et al.*, *supra* note 160. As noted, we submit those comments separately to this record, for the Commission's convenience.

dimension in a merger matter, it has found that consideration fruitless.[197] There are good reasons for this lacuna in the Commission's long and vigorous enforcement history.[198] The notion that the Commission would consider adopting broad rules to remedy supposed competitive harms in an area in which it has brought zero cases strains credulity. And that is independent of the contested question regarding whether the Commission's Section 6 competition rulemaking authority does or does not contemplate substantive or "legislative" rules and not just procedural ones.[199]

Nevertheless, some continue to advocate that privacy issues should often be considered in antitrust analyses.[200] Nothing in the foregoing proves that there are no facts and circumstances under which privacy issues would figure significantly in a competition action. But the mere possibility of competition issues does not demonstrate a pattern of harmful conduct or antitrust violations—far from it. Here, we briefly review some of the issues raised in our prior comments, with a focus on nonprice competition in particular.

1. Privacy as a nonprice dimension of competition

Discussions of privacy as an antitrust matter commonly focus on it as a nonprice dimension of competition in product or services markets—that is, as a material qualitative attribute. Thus, some have argued that "privacy harms can lead to a reduction in the quality of a good or service, which is a standard category of harm that results from market power. Where these sorts of harms exist, it is a normal part of antitrust analysis to assess such harms and seek to minimize them."[201]

Abstracted from privacy and data-security issues, we note that the Horizontal Merger Guidelines have long recognized that anticompetitive effects may "be manifested in nonprice terms and conditions that adversely affect customers."[202] In some contexts, this is workable in practice. As the United States observed in a note to the OECD on nonprice effects of mergers, "FTC enforcement actions involving competing hospitals typically involve consideration of a number of nonprice effects, such

---

[197] Statement of Fed. Trade Comm'n Concerning Google/DoubleClick, FTC File No. 071-0170, 2-3 (Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf; *see also* Geoffrey A. Manne & Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRONICLE 9 (May 2015), https://ssrn.com/abstract=2617685.

[198] For a general discussion, see, *e.g.*, Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121 (2015).

[199] *Compare, e.g.*, Thomas W. Merrill & Kathryn T. Watts, *Agency Rules with the Force of Law: The Original Convention*, 116 HARV. L. REV. 467, 505-09, 586 (2002); *with* Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. CHI. L. REV. 357 (2020).

[200] *See, e.g.*, Laura Alexander, *Privacy and Antitrust at the Crossroads of Big Tech*, American Antitrust Institute (2021), https://www.antitrustinstitute.org/work-product/aai-issues-report-antitrust-and-privacy.

[201] Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, Center for American Progress (Oct. 19, 2007), https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis; *see also* Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769 (2010).

[202] Horizontal Merger Guidelines of the U.S. Dep't of Justice and the Fed. Trade Comm'n, 2 (2010), https://www.ftc.gov/system/files/documents/public_statements/804291/100819hmg.pdf.

as investments in health information technology, advancements in disease management, and clinical integration."[203]

In certain health-care markets, the competitive significance of certain elements of nonprice competition is well-studied and, to a useful extent, understood. For example, in *Penn State Hershey Medical Center*, the Commission alleged that the merger would eliminate the provider's incentives to continue efforts to modernize, expand oncology services, and construct a new outpatient facility.[204] FTC staff have also conducted retrospective studies of consummated hospital mergers indicating that mergers of significant hospital competitors can result in reductions in important measures of clinical quality, such as mortality or surgical complications.[205]

In most contexts, however, such nonprice analysis presents significant problems in application.[206] First, product-quality effects can be extremely difficult to distinguish from price effects. Quality-adjusted price is usually the touchstone by which antitrust regulators assess prices in competitive-effects analyses. Or, to put it another way, the price signal regards not just a monetary price but information about product or service quality, convenience, etc. But disentangling (allegedly) anticompetitive quality effects from simultaneous (neutral or procompetitive) price effects is often an imprecise exercise, at best. For this reason, proving a product-quality case alone tends to be very difficult and requires connecting the degradation of a particular element of product quality to a net gain in advantage for the monopolist.

Second, product quality is often multi-dimensional. Even in a relatively simple case, product quality could include, for example, both function and aesthetics. Automobiles come in different styles and colors, offer seating for two, four, or more, and often allow a consumer to choose between power and mileage, or between different energy sources. Of his "Model-T," Henry Ford famously quipped

---

[203] U.S. Submission on the Nonprice Effects of Mergers, DAF/COMP/WD(2018)45 (May 30, 2018), https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/non-price_effects_united_states.pdf.

[204] *In re Penn State Hershey Medical Center*, Dkt. 9368 (complaint filed Dec. 14, 2015), https://www.ftc.gov/enforcement/cases-proceedings/141-0191/penn-state-hershey-medical-centerpinnaclehealth-system. For other health-care mergers involving nonprice analyses, see also *In re Advocate Health Care Network, et al*, Dkt. 9369 (complaint issued Dec. 18, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/141-0231/advocate-health-care-network-advocate-health-hospitals; *In re Sanford Health*, Dkt. 9376 (complaint filed Jun. 22, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/171-0019/sanford-healthsanford-bismarckmid-dakota-clinic.

[205] *See* Patrick S. Romano & David J. Balan, *A Retrospective Analysis of the Clinical Quality Effects of the Acquisition of Highland Park Hospital by Evanston Northwestern Healthcare*, 18 INT'L J. ECON. BUS. 45 (2001); Deborah Haas-Wilson & Christopher Garmon, *Two Hospital Mergers on Chicago's North Shore: A Retrospective Study*, 18 INT'L J. ECON. BUS. 17 (2011). Other studies analyzing nonprice effects of mergers include Gregory J. Werden, Andrew S. Joskow & Richard L. Johnson, *The Effects of Mergers on Price and Output: Two Case Studies from the Airline Industry*, 12 MANAGERIAL & DECISION ECON. 341 (1991); Steven Berry & Joel Waldfogel, *Do Mergers Increase Product Variety? Evidence from Radio Broadcasting*, 116 Q.J. ECON. 1009 (2001); Andrew Sweeting, *The Effects of Mergers on Product Positioning: Evidence from the Music Radio Industry*, 41 RAND J. ECON. 372 (2010); B.P. Pinto & D.S. Sibley, *Unilateral Effects with Endogenous Quality*, 49 REV. INDUS. ORG. 449 (2016); K.R. Brekke, L. Siciliani, & O.R. Straume, *Horizontal Mergers and Product Quality*, 50 CANADIAN J. ECON. 1063 (2017).

[206] For a full discussion of this problem, *see* Manne & Sperry, *supra* note 197.

that "any customer can have a car painted any color that he wants so long as it's black."[207] Today, Ford offers numerous models in an array of colors, with gasoline, hybrid, and electric-powered engines on offer. For example, the 2022 Ford Mustang automobile is available in 10 different versions or "models."[208] One of the least expensive, the "eco-boost fastback" version, can be obtained in any of 12 basic exterior colors, with additional choices available on roof, trim, and interior colors. Additional choices abound, ranging across functional attributes (engine size, tires, etc.) and decorative ones. The various choices may be valued differently by different consumers, although most of the available choices have market prices. Where there is no such price or an established proxy, a nonprice-effects analysis involving product quality across multiple dimensions can become exceedingly difficult—especially if there are tradeoffs in consumer welfare across those dimensions. Any such analysis would necessarily involve a complex and imprecise comparison of the relative magnitudes of harm and benefit to consumers who prefer one type of quality to another.

Privacy, as we have seen, is just such a complex case. It also involves both functional and subjective elements, and often a far richer set of tradeoffs and far less clarity about how to assess or order them. And, as discussed above, there may be tradeoffs among privacy values or between privacy and data-security values.

Finally, recent empirical evidence undermines the intuition that large dominant firms might tend to exploit their market power to diminish privacy (and hence, in effect, to suppress product or service quality). Using data from PrivacyGrade.org—which provides a privacy grade or rating for each app in the Android app marketplace, along with metrics for app quality and usage—Cooper & Yun find "no relationship… between privacy grades and our proxies for market power—market shares… and market concentration."[209] They also find "a negative relationship between privacy levels and quality ratings, suggesting a tradeoff between privacy and other dimensions of product quality that consumers value."[210] Analysis of alternative web-traffic data and a competing source of privacy ratings also fails to find a relationship between privacy ratings and market shares or concentration.[211]

---

[207] B. JOSEPH PINE II, MASS CUSTOMIZATION: THE NEW FRONTIER IN BUSINESS COMPETITION (1993) at 7; *The Model T*, FORD CORPORATE (*last visited* Nov. 9, 2022), https://corporate.ford.com/articles/history/the-model-t.html ("While Henry Ford did say 'Any customer can have a car painted any color that he wants so long as it's black,' the policy was in place solely for efficiency and uniformity.").

[208] *See 2022 Mustang*, FORD.COM (*last visited* Nov. 9, 2022), https://shop.ford.com/configure/mustang/config/paint/Config%5B%7CFord%7CMustang%7C2022%7C1%7C1.%7C100A.P8T..PM7...COU.EBST.LESS.%5D?gnav=shopnav-bp.

[209] James C. Cooper & John M. Yun, *Antitrust and Privacy: It's Complicated*, Vol. 2022 U. ILL. J.L. TECH. & POL'Y 343, 348 (2022).

[210] *Id.*

[211] *Id.* (examining website-traffic data from SimilarWeb and privacy ratings from DuckDuckGo for sites in 37 categories).

2. *Additional competition issues*

Additional competitive concerns have been raised about data, but as explained in detail in our prior Hearings comments.[212] none of these support a general analysis of net harmful conduct.

a. 'Big Data,' bigger data, and concerns about scale and scope

Some have questioned whether data—big[213] or otherwise—might constitute a barrier to entry.[214] In special cases, it might, as demonstrated by some of the FTC's own data-competition matters. But those cases all depended on unique qualitative features of particular datasets, for which—on FTC staff's analysis—there were no available substitutes or no viable means to create them.[215] None turned on some simple general feature of a dataset, such as its size or scope. Data is collected, stored, and analyzed because it has value. But it doesn't have fixed value: some datasets are more valuable than others, depending on the nature of the data, its source, and its application.[216] Some datasets—or close substitutes—are readily obtained, and some are not. Some data rapidly grow stale, and some have more enduring value.[217] As an FTC representative explained at the hearings, data markets are dynamic, and "[d]ata markets and sets are highly differentiated. Each investigation looks very closely at the specific facts of the case.[218]

---

[212] Auer, *et al.*, *supra* note 186.

[213] Numerous writings have tried to capture key aspects of the expansion of data collection, analysis, and use under the rubric "big data." Although there is no uniform definition of "big data," there is widespread interest in what is sometimes referred to as "the four Vs": "Big Data consists of extensive datasets—primarily in the characteristics of volume, variety, velocity, and/or variability—that require a scalable architecture for efficient storage, manipulation, and analysis." NIST Big Data Interoperability Framework, V. 1: Definitions, NIST Big Data Public Working Group (2018), https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1r1.pdf; *see also*, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf ("The term 'big data' refers to a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions").

[214] *Compare, e.g.*, Robert Mahnke, *Big Data as a Barrier to Entry*, COMP. POL'Y INT'L (May 29, 2015), https://www.competitionpolicyinternational.com/assets/Uploads/Mahnke2May-152.pdf ("The fact that "big data" can be an antitrust relevant barrier to entry has been well established."), *with* Daniel L. Rubinfeld & Michel S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339, 380-81 (2017) (recognizing that "much depends on case-specific facts" and that "[t]he collection and analysis of big data has undoubtedly increased social welfare," while concluding that "big-data markets are also often characterized by entry barriers, which, in turn, have the potential to create durable market power in data-related markets or to serve as a basis for anticompetitive conduct").

[215] *See, e.g.*, Testimony of Haidee Schwartz, FTC Bureau of Competition, Fed. Trade Comm'n Hearings on Big Data, Privacy, and Competition, *supra* note 195, Tr. 266; U.S. Note to OECD, Data Rights and Competition, *supra* note 162.

[216] *See generally*, *e.g.*, Anja Lambrecht & Catherine Tucker, *Can Big Data Protect a Firm from Competition*, CPI ANTITRUST CHRONICLE (2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/01/CPI-Lambrecht-Tucker.pdf; Hal Varian, *Artificial Intelligence, Economics, and Industrial Organization*, *in* THE ECONOMICS OF ARTIFICIAL INTELLIGENCE: AN AGENDA 15 (Ajay Agrawal, Joshua Gans & Avi Goldfarb eds., 2018).

[217] *Id.*

[218] Testimony of Haidee Schwartz, *supra* note 241, at Tr. p. 279.

b. Zero-price goods and services and consumer privacy preferences

Some critics suggest that special problems arise from business models that offer consumers free services supported by the monetization of consumer data gathered in connection with consumer access to those services.[219] On the one hand, antitrust tends to favor low prices (all else equal), as do consumers, and zero is a very low price. That does not bar antitrust concerns, as we have seen with nonprice competition. But as discussed above, the difficulty of parsing price and quality effects is especially present in privacy matters. Moreover, there can be tradeoffs between *improvements* in product quality that are derived from increased or ongoing data collection and demonstrated, likely, or purported privacy harms. As we have seen, the marginal privacy risk to consumers associated with any given data-collection and use practice may be indeterminate or hard for expert agencies, much less consumers, to assess. In addition, a decrease in privacy protection along one or more dimensions of privacy may not be a simple transfer from consumers to producers. Consumers can benefit from, for example, reduced search costs and increased relevance or accuracy of information retrieval, which may derive more detailed tracking by a provider such as a search engine or a mapping service.[220] The collection and use of data by a company like Google can be used to improve the quality of the company's products along several dimensions material to consumers. Improving product quality while maintaining a constant zero price—*i.e.*, decreasing quality-adjusted price—is not normally an antitrust injury.

Where there are tradeoffs, the positive value consumers derive from online content is a baseline consideration.[221] In addition, available data suggests that many consumers value low prices and nonprivacy attributes of goods and services more highly than privacy.[222] For example, consumers tend to choose free, ad-supported apps over 99-cent alternatives without ads.[223]

---

[219] *See, e.g.*, Michal S. Gal & Daniel L. Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement*, 80 ANTITRUST L.J. 521 (2016).

[220] Diana I. Tamir & Jason P. Mitchell, *Disclosing Information About the Self Is Intrinsically Rewarding*, 109 PROC. NAT'L ACAD. SCI. (PNAS) 8038 (2012); Acquisti, *et al.*, *supra* note 67, at 445; Cooper & Yun, *supra* note 209, at 347-48.

[221] For example, Brynjolfsson, Collis, & Eggers use a combination of survey methodologies to show that high levels of consumer surplus are associated with free online content. Erik Brynjolfsson, Avinash Collis & Felix Eggers, *Using Massive Online Choice Experiments to Measure Changes in Well-being*, 15 PROC. NAT'L ACAD. SCI. 7520 (2019) (using willingness-to-accept estimates to show that the median consumer in 2016 valued online search at $14,760 per year and valued the rest of the Internet at $10,937 per year, or roughly $8.3 trillion in aggregate for the United States). *See also*, Leonard Nakamura, *et al.*, *"Free" Internet Content: Web 1.0, Web 2.0, and the Sources of Economic Growth*, Fed. Reserve Bank of Philadelphia Working Papers, WP 18-17 (2018), https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-17.pdf (analyzing contribution of "free" content to domestic production, and estimating addition of $294 billion to U.S. GDP, based on cost of production).

[222] *See, e.g.*, Alastair R. Beresford, Dorothea Kübler, & Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* (SFB 649 Discussion Paper 2011-010, 2011), *available at* http://edoc.hu-berlin.de/series/sfb-649- papers/2011-10/PDF/10.pdf; Jens Grossklags & Alessandro Acquisti, *When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, in Proceedings of the Sixth Workshop on the Economics of Information Security (2007), *available at* http://weis2007.econinfosec.org/papers/66.pdf.

[223] Mary Ellen Gordon, *The History of App Pricing, and Why Most Apps are Free*, THE FLURRY BLOG (Jul. 18, 2013), http://blog.flurry.com/bid/99013/The-History-of-App-Pricing-And-Why-Most-Apps-Are-Free.

> the available empirical evidence suggests that, although consumers profess to care deeply about privacy, they do not tend to alter their consumption choices based on privacy concerns. There are various explanations for the privacy paradox, but the underlying cause is irrelevant—if consumers do not respond to firms' privacy choices, privacy cannot be an important dimension of competition.[224]

To make out a competition case, enforcers would have to consider the relative magnitudes of diverse benefits and harms broadly, and not just perceived harms to what might well be a relatively small group of privacy-sensitive consumers (who have not otherwise protected themselves by use of marketplace tools like track blockers or by use of opt-out options provided by major ad networks and data brokers). To conduct the analysis in a particular case would be challenging. To make out a general case for regulation, across business models and varieties of commercial-data usage, would be vastly more difficult, and a fundamental challenge to regulatory proposals.

C. Price Discrimination as a Privacy Harm

Some have argued that "big data"—or data collection and usage by large firms such as Google and Facebook—facilitates price discrimination,[225] and that price discrimination can harm consumers in ways cognizable as antitrust injuries. That is, because companies like Google and Facebook collect a great deal of consumer data, they or other firms could segment groups based on certain characteristics and offer them different deals. The resultant price differentiation—or "price discrimination"—could entail that many consumers pay more than they would in the absence of the data collection. The welfare of those consumers would be diminished.

This argument, however, misses a large part of the story. Price discrimination is differential pricing instead of a uniform market price: prices are lower for some consumers just as they are higher for others, a possibility explored by the White House Report on Big Data and Differential Pricing.[226] More generally, the effect of price discrimination on welfare is indeterminate in the abstract, and it can be welfare enhancing on net when it is accompanied by an increase in output.[227]

There are additional challenges. First, absent significant barriers to entry, supracompetitive profits are unlikely to be durable. Such profits inevitably attract entry from competitors and/or encourage consumers to switch toward rival firms or to substitute goods or services.

---

[224] Cooper & Yun, *supra* note 209, at 347 (internal citations omitted).

[225] *See* Maurice E Stucke, *Should We Be Concerned About Data-opolies?*, 2 GEO. L. TECH. REV. 275, 293 (2018). *See also,* Curtis R Taylor, *Consumer Privacy and the Market for Customer Information*, RAND J. ECON. 631 (2004).

[226] *The Economics of Big Data and Differential Pricing*, EXEC. OFFC. OF THE PRESIDENT, 2, 4-6 (February 2015), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf.

[227] Acquisti & Varian show that the conditions under which such price discrimination is profitable for a monopolist vary. In their baseline model, involving rational consumers with constant valuations and a monopoly merchant who can commit to a pricing policy, they show that, "although it is feasible to price so as to distinguish high-value and low-value consumers, the merchant will never find it optimal to do so." Alessandro Acquisti & Hal R. Varian, *Conditioning Prices on Purchase History*, 24 MKTNG. SCI. 367 (2005).

Second, even if a firm could price discriminate without the threat of arbitrage, high-value consumers would still have huge incentives to withhold their personal information and/or send deceptive signals that they are low-value purchasers. When this is the case, the ability to acquire detailed consumer information may, counterintuitively, lead to lower prices and higher consumer welfare.[228]

More broadly, while some have focused on the possible negative effects of price discrimination to one subset of consumers, they generally ignore the positive effects of businesses being able to expand output by serving previously underserved consumers. A profit-maximizing monopolist that can expand output and partition consumers has an incentive to serve consumers with a lower willingness to pay—commonly, lower-income consumers—as long as willingness to pay exceeds the marginal cost of production.[229] While some research suggests that price discrimination *can be* a net harm in some narrow circumstances,[230] many other studies find that consumers benefit from more price discrimination. For example, in a randomized control trial involving a large digital firm and its customers, Dube & Misra find that "60% of consumers benefit from lower prices under personalization" of prices.[231] In another study using eBay data, when sellers are able to use "detailed information on individual web–browsing and purchase histories" that was previously unimaginable for sellers, with price discrimination "a significant fraction of consumers are better off under price discrimination relative to uniform pricing, as price discrimination intensifies competition for each individual consumer."[232] Even in the face of laws preventing direct price discrimination, indirect attempts at price discrimination can help consumers and lower prices.[233]

Under certain conditions, price discrimination based on detailed consumer data can mitigate competitive harm. For example, Cooper, *et al.*, use a microeconomic model to study spatial price discrimination, contrasting three-to-two mergers when firms do and do not have access to detailed consumer information.[234] Their analysis suggests that access to detailed consumer information and the ability to set prices conditioned on that information may cause a merger to have less of an anticompetitive price effect than if firms lacked this information or the ability to charge anything but uniform prices.

---

[228] *See* Taylor, *supra* note 225, at 643.

[229] Regarding price discrimination, output, and consumer welfare, see, *e.g.*, Richard Schmalensee, *Output and Welfare Implications of Monopolistic Third-degree Price Discrimination*, 71 AMER. ECON. REV. 242 (1981); Hal R. Varian, *Price Discrimination and Social Welfare*, 75 AMER. ECON. REV. 870 (1985).

[230] *See* Mark Armstrong & John Vickers, *Discriminating Against Captive Customers*, 1 AM. ECON. REV. INSIGHTS 257 (2019).

[231] Jean-Pierre Dube and Sanjog Misra, *Personalized Pricing and Consumer Welfare*, J. POL. ECON. (forthcoming).

[232] Patrick J. Kehoe, Bradley J. Larsen, and Elena Pastorino, *Dynamic Competition in the Era of Big Data*, Stanford University Technical report (2018).

[233] For example, see Julie Holland Mortimer, *Price Discrimination, Copyright law, and Technological Innovation: Evidence from the Introduction of DVDs*, 122 Q. J. ECON. 1307 (2007).

[234] James C. Cooper, Luke M. Froeb, Daniel P. O'Brien & Steven Schantz, *Does Price Discrimination Intensify Competition? Implications for Antitrust*, 72 ANTITRUST L.J. 327 (2004-05).

D. Data monopolies

Some allege that regulatory intervention in markets involving data is necessary because these markets, driven by "data network effects," tend to create unassailable monopolies.[235] A closer inspection of numerous digital markets, however, suggests that this concern is overstated.

For a start, it is wrong to assume that data-intensive products necessarily lead to winner-take-all situations, akin to those that may occur in the presence of network effects. As Hal Varian aptly demonstrates, unlike network effects, data does not produce value in and of itself.[236] Instead, data must be analyzed to create value. As a result, companies cannot merely outcompete their rivals by acquiring superior or larger datasets: they must also hire the best data engineers and "learn by doing."[237] Because of this, there is no necessary data "positive feedback loop" and an industry's heavy reliance on data does not necessarily lead to higher concentration.

Even where there are network effects, there is little reason to believe that this would make data-reliant markets less competitive. Although some scholars have voiced fears that network effects may lead to highly concentrated markets, not all markets with network effects will eventually tip toward a single winning firm. Moreover, in those cases where network effects do lead to lopsided market distributions, potential competition from smaller competitors or new entrants may constrain the behavior of incumbents. In this case, the presence of network effects might merely substitute competition "in the market" with competition "for the market."[238]

These dynamics can lead to firm behavior that protects users' privacy. In a highly acclaimed paper, Mark Armstrong has shown that competition between multi-sided platforms may result in particularly intense competition to acquire single-homing users (who are present on only one of many competing platforms).[239] This is often, though not always, the case for users of social networks, search engines, game consoles, and online retail platforms. Because there will be intense competition to attract these exclusive consumers (often resulting in zero nominal prices), any latent demand for privacy protection is likely to be met by competing firms.

There is thus little reason to believe that the presence of network effects would necessarily lead to inferior privacy protections for users. On the contrary, as has already been mentioned, network

---

[235] *See* Stucke, *supra* note 225, at 283.

[236] *See* Hal Varian, *Artificial Intelligence, Economics, and Industrial Organization*, *in* THE ECONOMICS OF ARTIFICIAL INTELLIGENCE: AN AGENDA 15 (2018).

[237] *Id.*

[238] *See* Sami Hyrynsalmi, Arho Suominen & Matti Mäntymäki, *The Influence of Developer Multi-homing on Competition Between Software Ecosystems*, 111 J. SYS. & SOFTWARE 119, 119-27 (2016).

[239] *See* Mark Armstrong, *Competition in Two-sided Markets*, 37 RAND J. ECON. 678 (2006).

effects are a double-edged sword that are likely to result in platforms catering closely to the needs of privacy-conscious users and thus benefiting all other users on the network.[240]

Moreover, there is reason to believe that the competitive process itself is fully capable of protecting privacy interests. In their empirical study of consumer preferences and firm behavior with respect to consumer-privacy protections, Tsai, *et al.*, found that:

> businesses may use technological means to showcase their privacy-friendly privacy policies and thereby gain a competitive advantage. In other words, businesses may direct their policies and their information systems to strategically manage their privacy strategies in ways that not only fulfill government best practices and self-regulatory recommendations, but also maximize profits.[241]

Further, particularly in markets characterized by high degrees of technological change, potential competition can operate as effectively as—or even *more* effectively than—actual competition to generate competitive market conditions:

> [I]n industries... where technological change is rapid, competition for the market may provide more benefits to consumers than competition in the market. Where competition for the market is important, the number of competitors in the market at any point does not usefully measure the extent to which competitive processes underlie market behaviour.[242]

As applied here, if privacy-protections are important to consumers, firms in technology-heavy industries that are competing for the market have a sharp interest in meeting that consumer demand. The fact that, at any given time, only a single firm or only a few firms constitute an industry does not mean that the industry is not responsive to consumers' preferences for privacy, as it is for all other aspects of the products and services they consume.

Conclusion

The Commission and its staff have made important contributions to consumer privacy and data security under both special statutory charges and general application of Section 5. Those contributions are aptly cited in the ANPR. It is unfortunate, however, that the ANPR does not frame the FTC's considerable experience in a way that can foster useful and focused discussion on the question

---

[240] *See* David S. Evans & Richard Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses*, in OXFORD HANDBOOK OF INTERNATIONAL ANTITRUST ECONOMICS 405 (Roger Blair & Daniel Sokol eds., 2013).

[241] Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 266 (2011).

[242] Neil Quigley, *Dynamic Competition in Telecommunications: Implications for Regulatory Policy* 17, C.D. HOWE INSTITUTE COMMENTARY No. 194 (February 2004), *available at* https://www.cdhowe.org/pdf/commentary_194.pdf. *See also* A.E. Kahn, *Telecommunications: The Transition from Regulation to Antitrust*, 5 J. TELECOMM. & HIGH TECH. L. 159 (2006); Jason Pearcey & Scott J. Savage, *Actual and Potential Competition in International Telecommunications* 4 (Working Paper, Oct. 21, 2015), *available at* https://www.montana.edu/jpearcy/papers/ISR_Web.pdf ("Overall, these results suggest that incumbent firms reduce their price when potential competition increases....").

of whether certain additional data regulations are needed, or if so, whether they might be adopted under the FTC Act. The central defect of the ANPR is its failure to satisfy even the basic and preliminary requirements for an ANPR under Section 18 of the FTC Act. By providing a sweeping but open-ended definition of an unestablished term ("commercial surveillance"), the Commission has failed to identify with any clarity the types of commercial conduct at-issue. Without a type of conduct, it is difficult to identify a "pattern" of it, as required under Section 18.

Regulation and enforcement under the Commission's "unfairness" authority both require a type of cost-benefit analysis, accounting for consumer-welfare and competitive effects. Harms or injuries addressed must be substantial and not reasonably avoided by consumers themselves, and they must not be outweighed by countervailing benefits to consumers. In brief, do not prosecute conduct that does more good than harm. While the ANPR acknowledges those basic commitments, it fails to account for them. By suggesting an open-ended "small fraction" of diverse or disparate harms—some clear but some vague or ambiguous, some subject to measurement or estimation and some not, some plainly actionable under Section 5 and some not—and by barely nodding to the myriad benefits provided by the digital economy, the Commission has simply failed to specify the very subject matter of a potential rulemaking. What harms are to be diminished, what conduct regulated, and by what means? Section 18 requires a description of the Commission's objectives. What are they? Section 18 requires a description of regulatory alternatives under consideration. What are they?

Asking questions and seeking input are critical to rulemaking under either Section 18 or the APA. They are also central to the Commission's research and advisory missions under Section 6 of the FTC Act. But asking nearly 100 disparate and compound questions simply calls to mind a platitude: sometimes, less is more. Some of the questions are useful, and we do not doubt that some useful materials will be submitted to the record of this proceeding. What is unlikely is a coherent set of submissions.

Rather than advance a rulemaking, the ANPR suggests important work that the Commission should undertake before considering data regulation under any of its authorities. The following projects would be useful, and well within the Commission's competence. First, while the ANPR proffers an open-ended list of potential harms, it does not present the Commission's current thinking about informational injuries that are cognizable under the FTC Act. The Commission has decades of enforcement experience addressing those harms, and the Commission and its staff have undertaken considerable economic and policy research pertinent to privacy and data-security enforcement. A clear up-to-date assessment of the Commission's current understanding of informational injury, and of how to assess or estimate such injuries, would be of great value to industry, lawmakers, and the public.

Second, clear guidance on the Commission's current understanding of how informational injuries should be addressed under Section 5 "UDAP" authority could also be of tremendous benefit to industry, lawmakers, and the public. Such guidance would, of necessity, account for the assessment of countervailing benefits too.

The Commission's enforcement experience should be a key input into these projects. In addition, contributions of the FTC's Bureau of Economics could be invaluable, not least because the Bureau employs experts in both consumer-protection and industrial-organization economics, and it has expertise applying serious research to specific enforcement problems. That suggests a third task contemplated by the ANPR itself: there is a considerable and growing body of research on the impact of privacy, data security, and general data regulations on consumers and competition. That research is important and informative, but it is not remotely comprehensive. First, the question of benefits to consumers and competition produced by data regulations has been radically understudied. And while there is much more evidence of regulatory costs, more work could be done in that area too.

Commission staff are well-qualified to undertake a critical synthesis of the extant body of research, commence new studies, and help foster more research by third parties in academia and industry. There is simply no prospect of a serious cost-benefit analysis for any proposed data regulations without further development of the field. Moreover, considering the skew toward evidence of consumer and competitive costs associated with extant data regulations, the Commission should be wary of regulatory initiatives that run ahead of the state of knowledge.

Some of these projects might have been completed under the Commission's prior rules regarding procedures for Magnuson-Moss rulemaking. In July 2021, without public comment, the Commission revised its rules of practice for Section 18 rulemaking, among other things.[243] At that time, the Commission chose to "eliminate the requirement that Commission staff publish a staff report containing an analysis of the rulemaking record and recommendations as to the form of the final rule for public comment."[244] The consequences of that rule change are reflected unfortunately in the ANPR, to the detriment of the public, Congress, and the rulemaking process. At least some of the analyses and reporting strikingly absent from the ANPR would very likely have been included in such a staff report and which, under prior agency rules, would have been submitted to an independent presiding officer.[245] Moreover, the dearth of empirical evidence and economic analysis reflected in the ANPR would be hard to imagine under the prior process, which required as a preliminary matter that staff consult "economic, business, and trade journals," among other things.[246] The prior rules also required an "initial staff report,"[247] and review by the Bureau of Economics, which would

[243] Revisions to Rules of Practice, Fed. Trade Comm'n, 86 FED. REG. 38542 (Jul. 22, 2021) (codified at 16 C.F.R. Parts 0 & 1)

[244] *Id.* at 38544.

[245] As the Commission is aware, Section 18 requires that an officer preside over rulemaking proceedings, and that the officer report to a "chief presiding officer who shall not be responsible to any other officer or employee of the Commission." 15 U.S.C. § 57a(c)(1)(B).

[246] Fed. Trade Comm'n, OPERATING MANUAL (1989), Procedures for Magnuson-Moss Rulemaking, Ch. 7.3.5.4.2., *available at* https://web.archive.org/web/20180123162242/https://www.ftc.gov/about-ftc/foia/foia-resources/ftc-administrative-staff-manuals.

[247] *Id.* at 7.3.8.1.1; 7.3.10.3.2.

either concur in staff recommendations or issue a separate memorandum outlining the Bureau's objections and its own recommendations.[248]

The Commission has also enquired about intervention under its competition authority. As we describe above in some detail, nonprice dimensions of competition can be important, but they can be difficult to assess in many circumstances, and perhaps especially difficult in privacy matters. Privacy has not yet been decisive in a merger or anticompetitive-conduct matter, and there are good reasons for this lacuna in the Commission's record. There are no good grounds for adopting general regulations given this enforcement history.

Also sketched above, and discussed in greater detail in a separate submission, are questions about consumer data as an asset (or production input). Those comments counsel caution on various issues. In closing, we add one note: the Commission's data cases have all focused on distinctive—often unique—datasets with distinctive applications. Those cases all depend heavily on special facts and circumstances. There are likely to be more such cases in the future, but the particularity of the Commission's successful rule-of-reason competition cases involving data militate in favor of continued case-by-case enforcement, and against general data regulations.

To be sure, uniform federal privacy or data-security regulations of the right type could be effective, efficient, and on net beneficial. In addition to ameliorating unaddressed harms, such regulations could serve to clarify and simplify the regulatory landscape, reducing the costs of regulatory complexity and uncertainty, and educating consumers as well as industry. We expect that the prospects of focused and grounded data-security regulations exceed those of privacy regulations or, at least, are likely to precede them. In any case, as we have discussed, data regulations entail complex tradeoffs, some of which are more the purview of Congress than an expert enforcement agency. And the Commission's expertise and statutory mission both suggest—indeed require—critical research and reporting tasks to be advanced before considering regulation.

[248] *Id.* at 7.3.8.3.