**Executive Summary of Comments of the International Center for Law & Economics**

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

***Federal Trade Commission Docket No. FTC-2022-0053***

*October 20, 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)

**Executive Summary of Comments of the International Center for Law & Economics, Advance Notice of Proposed Rulemaking on Trade Regulation Rule on Commercial Surveillance and Data Security**

*October 2022*

**Geoffrey A. Manne, Daniel Gilman, & Kristian Stout[[1]](#footnote-2)\***

# Introduction

The Federal Trade Commission (“FTC”) has issued an Advanced Notice of Public Rulemaking (“ANPR”) on “Commercial Surveillance and Data Security,”[[2]](#footnote-3) 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.”[[3]](#footnote-4) On some possible approach, 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; and its enforcement experience 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 Commission’s authority is not unbounded, however, and neither are its resources. Both limitations become 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 adopt, the kinds of sweeping data regulations that the Commercial Surveillance ANPR appears to contemplate.

# 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,[[4]](#footnote-5) 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”).[[5]](#footnote-6) Rulemaking under Section 18 of the FTC Act[[6]](#footnote-7) requires that the Commission follow a careful process: as a preliminary matter, it must identify, for 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.[[7]](#footnote-8) 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”[[8]](#footnote-9) 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.[[9]](#footnote-10)

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.”[[10]](#footnote-11) 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.”[[11]](#footnote-12)

# 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. 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.

Irrespective of the statutory obligations to do so, this is also good procedure for policymaking. Before engaging in a deeply interventionist regulatory experiment—such as imposing strict privacy regulations in contravention of revealed consumer preferences—there should be empirically justified reasons for doing 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 what problems the rules are needed to address. Without knowing their purpose, any rules are likely to be ineffective, at best, and harmful, at worst. They may increase costs for consumers and businesses alike; mandate harmful prescriptions for alleged privacy harms; or exacerbate the risks of harm—or all of the above. Whether such costs would be accompanied by concrete gains material to most consumers is also up for grabs.

Particularly in the United States, where privacy is treated both legally and socially as more of a consumer preference (albeit perhaps a particularly important one) than a fundamental right,[[12]](#footnote-13) it is difficult to determine whether our current regime produces the “right” amount of privacy protection. It is surely not sufficient to make that determination, however, that privacy advocates and consumers who are particularly privacy-sensitive think 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 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.

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]](#footnote-14) it is functionally described 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]](#footnote-15) 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 the ability of firms to ensure data security. The EU’s experience with the General Data Protection Regulation (“GDPR”) has demonstrated some of this dynamic.[[15]](#footnote-16) 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, 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.

# 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 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 mandates. 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.

The Commercial Surveillance ANPR does not specify, or even sketch, the data regulations being contemplated by the Commission as 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 large firms and incumbents.[[16]](#footnote-17)
* Second, studies of specific domestic-privacy and data-security requirements underscore the potential for unintended consequences, including competitive costs.[[17]](#footnote-18)
* 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]](#footnote-19)

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 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.

# 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, there already exist generally applicable laws at both the federal and state level that provide a wide scope of protection for individuals, including consumer-protection laws that apply to companies’ data use and security practices,[[19]](#footnote-20) as well as those that have been developed in common law (property, contract, and tort) and criminal codes.[[20]](#footnote-21) 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]](#footnote-22)

Despite the FTC’s noted experience in a certain slice of privacy regulation, Congress has not made the FTC the central privacy regulatory body. Congress has wrestled with complex tradeoffs in several different areas and has allowed—through design and otherwise—various authorities to emerge in this area. Thus, given the Supreme Court’s recent “major questions” jurisprudence,[[22]](#footnote-23) it is necessary to understand that the rules that emerge from this process must be properly constrained.

In his dissent from the issuance of this ANPR, Commissioner Noah Phillips noted the massive, 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]](#footnote-24)

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 seem 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 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.

1. \* 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. This executive summary is adapted from full comments that ICLE will submit to the Federal Trade Commission in November 2022. [↑](#footnote-ref-2)
2. 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”]. [↑](#footnote-ref-3)
3. *Id.* at 51277. [↑](#footnote-ref-4)
4. *Id.* at 51276. [↑](#footnote-ref-5)
5. 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). [↑](#footnote-ref-6)
6. 15 U.S.C. § 57a. [↑](#footnote-ref-7)
7. 15 U.S.C. § 57a(b)(2)(A). [↑](#footnote-ref-8)
8. 15 U.S.C. § 57a(a)(1)(B). [↑](#footnote-ref-9)
9. 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.”) [↑](#footnote-ref-10)
10. 15 U.S.C. § 57a(b)(2)(i). [↑](#footnote-ref-11)
11. 15 U.S.C. § 57a(b)(2)(ii). [↑](#footnote-ref-12)
12. Except, of course, when it comes to *government* access to private information, *i.e.*, under the Fourth Amendment. [↑](#footnote-ref-13)
13. See, *e.g.*, ANPR at 51273-75. [↑](#footnote-ref-14)
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. [↑](#footnote-ref-15)
15. *See, e.g.,* 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 and 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](https://ssrn.com/abstract%3D4030905) or <http://dx.doi.org/10.2139/ssrn.4030905>. [↑](#footnote-ref-16)
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 (Dec. 2019), *available at* <https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf>. [↑](#footnote-ref-17)
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). [↑](#footnote-ref-18)
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). [↑](#footnote-ref-19)
19. *See, e.g.*, FTC Act, 15 U.S.C. § 45(a) et seq. [↑](#footnote-ref-20)
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). [↑](#footnote-ref-21)
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. [↑](#footnote-ref-22)
22. *See, e.g.,* *W. Virginia v. Env’t Prot. Agency*, 142 S. Ct. 2587, 2595 (2022). [↑](#footnote-ref-23)
23. ANPR at 51293 (Dissenting Statement of Comm’r Noah J. Phillips). [↑](#footnote-ref-24)