Before the
Federal Trade Commission
Washington, D.C.

In re	File No. R111004
ANPR—Trade Regulation Rule on Commercial Surveillance and Data Security	

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Advance Notice of Proposed Rulemaking (the "ANPR") published in the Federal Register at 87 Fed. Reg. 51273 (Aug. 22, 2022), the Computer & Communications Industry Association ("CCIA")[1] submits the following comments:

I. Introduction

CCIA is pleased to participate in the Federal Trade Commission's consideration of whether it should adopt "new rules or other regulatory alternatives" addressing the collection, use, and transfer of consumer data.[2] ANPR at 1. We provide comment herein on several of the items raised in the ANPR, including the Commission's rulemaking and enforcement authority, the breadth of issues presented for comment, and the risk that overly prescriptive rules would impede innovation, hinder competition, and have a very limited lifespan.

The comments, however, question the Commission's authority to seek a broad, sweeping rulemaking on a topic that impacts almost every aspect of the modern economy. Congress delegated the FTC with narrow authority to engage in Section 18 rulemaking, subjecting the

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

[2] All citations to the ANPR refer to the long-form document released on August 11, 2022, rather than the edition published in the Federal Register.

process to substantive and procedural requirements.[3] Such broad authority is reserved for Congress, which is considering comprehensive privacy and security legislation. Furthermore, any proceeding undertaken pursuant to Section 5's authority to prohibit "unfair or deceptive acts or practices" must adhere to the statutory conditions that Congress has placed on the Commission's authority to identify unlawful conduct.

The Commission may declare an act or practice "unfair" if (1) the conduct "causes or is likely to cause substantial injury to consumers;" (2) that injury "is not reasonably avoidable by consumers;" and (3) the conduct carries no "countervailing benefits to consumers or to competition."[4] An act or practice is declared "deceptive" where it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers – that is, it would likely affect the consumer's conduct or decision with regard to a product or service. Of these criteria, the injury must be paramount, because by the statute's plain language the second and third criteria are irrelevant without injury.

The ANPR, however, seems to assume, rather than demonstrate, the presence, or at least the substantial risk, of injury caused by several commercial practices. These comments explain why those omissions are detrimental to the Commission's efforts in this proceeding. As the Commission progresses in its consideration of digital privacy, the demonstrable presence of harm, or at the least likelihood, should remain its touchstone with regard to each act and practice it reviews.

The ANPR also indicates a failure to appreciate the value of interpersonal communication and community that online, digital services enable. In the balancing of interests that this rulemaking would require, benefits to consumers must be given appropriate weight. Those benefits are often commercial – fast, reliable, efficient delivery of items chosen from a vast array of online retailers – but just as often they come in the form of improved mental and emotional well-being. Groups that feel marginalized, many of them teens and young adults, rely on apps and websites to feel supported and less alone. Rules that would hinder these persons' access to online resources free of charge could return them to feelings of isolation and lack of acceptance.

---

[3] The Commission can prescribe rules that define specific acts or practices that are unfair or deceptive only when the Commission has reason to believe "that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent." 15 U.S.C. § 57a(b)(3).

[4] 15 U.S.C. §45(n)

II. Discussion

These comments address several aspects of the ANPR, including the Commission's "overview" of the privacy landscape, ANPR at 2-14, the discussion of the Commission's authority, *id*. at 14-23, and many of the specific questions that the Commission sets forth for input, *id*. at 24-41.

A. "Surveillance" Is an Inappropriate and Overbroad Term for Referring to the Online, Digital Ecosystem.

The Commission's recent adoption of the word "surveillance" in connection with online services is troubling. The word suggests a nefarious purpose, as well as intent to police or sanction consumers and a clandestine mode of operation. Most of all, "surveillance" connotes a violation of rights and thus appears to presuppose the existence of actionable harm. Using this word attempts to short-circuit the Commission's Section 5 analysis, possibly inciting Commission action in the absence of satisfying the statutory predicates Congress set forth.

The interaction between consumers, publishers, advertisers, and digital services providers cannot reasonably be characterized as "surveillance". The Internet ecosystem is the greatest marketplace ever created, enhancing virtually every aspect of American life: commerce, information, health and well-being, community involvement, and education. It is an ecosystem for exchanging ideas, imparting knowledge and information, connecting buyers to sellers, and enabling the efficient provision of vital services. Individuals seek things out and the online digital sector helps them find what they seek. In this exchange, individuals willingly provide information, and that information makes their search faster, easier, and more accurate. This relationship is not "surveillance", it is the core of the Internet and, where all parties know what the rules of the road are, it is a balanced and fair ecosystem.

CCIA encourages the Commission to reject the term "surveillance" as a divisive, inflammatory, and inapt term for all practices contemplated by this proceeding. It would be more productive to discuss these matters as "consumer protection," "data privacy," and the like.

B. The Commission Should Not Address Consumer Privacy and Data Security in the Same Proceedings, Which Would Undermine the Trade-Offs Within Each Discipline and Impede Other Ongoing Government Efforts.

The Commission's rationale for the purported broad rulemaking fixates on harms that

may result from either, or both – the vagueness of the ANPR makes it difficult to ascertain – lax data security and "commercial surveillance." ANPR at 22. For example, the Commission discusses a scenario where a hacker causes both security and privacy-related harms, yet they are not necessarily related. ANPR at 23. Data security and privacy, while inter-related, are distinct concepts, each carrying unique considerations and combatting different risks.

1. Addressing Data Security Requires a Harmonized Approach Across Government, And Specific Technical Expertise to Lead Those Efforts.

The data security policy space is already very active, with agencies that have specific data security mandates and expertise, such as the Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology (NIST) actively working in this space. For example, Congress recently passed incident reporting legislation for critical infrastructure owners and operators (CISA is in the process of rulemaking to implement this legislation),[5] the Office of the National Cyber Director is developing a national cyber strategy,[6] and NIST is developing its Cybersecurity Framework 2.0.[7] Yet, the Commission's list of over 90 questions conflates data privacy with security, without acknowledgment of the ongoing work in this space or the technical expertise needed to effectively execute data security policies. Further, the ANPR fails to distinguish between consumer harms that are specific to data security and privacy, undermining the efforts each discipline tries to address and the relevant statutory requirements with each.

Information and data privacy is focused on the governance of the collected information, with an emphasis on ensuring that (1) the data's use, collection, and sharing adheres to the companies' policies and other commitments; and (2) the data's use, collection, and sharing does not harm consumers in ways that outweigh benefits to consumers and competition. This consists of balancing the trade-offs with certain types of data, including sensitive information that may be subject to existing regulations. Information security or cybersecurity is the protection of

[5] Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55830 (Sept. 12, 2022)
[6] David Jones, *National Cybersecurity Strategy to Debut Within Months, White House Official Says,* Cybersecurity Dive (Oct. 20, 2022) https://www.cybersecuritydive.com/news/us-cyber-strategy-chris-inglis/634585/
[7] NIST Workshop, Journey to the NIST Cybersecurity Framework 2.0 Workshop #1 (Aug. 17, 2022) https://www.nist.gov/news-events/events/2022/08/journey-nist-cybersecurity-framework-csf-20-workshop-1

information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[8] This consists of assessing what hardware and software a business use, firewalls and segmentation, and more nuanced considerations such as how differing encryption standard for goods and services its other products and its organizational security posture.

A security program will focus on mitigation in the event of a breach or incident, tailored to the unique threats and risks to each organization. One such helpful tool in developing such risk management is the NIST Cybersecurity Framework which identifies five core functions – Identity, Protect, Detect, Respond, and Recover – that comprise essential aspects of a cybersecurity program.[9] This guidance is one of many useful tools helping organizations manage and respond to cybersecurity risk. Businesses need to develop and support security plans that assess the risks of using certain data to account for different risks and vulnerabilities[10] – a cloud vendor's security and data program will differ greatly from a small advertising company but each can still achieve robust standards despite these differences. These risks can consist of monetary or IP theft, operational downtime, and general mitigation efforts. A business can remediate some of the damages and security harms through adherence to breach notification requirements, as required in all 50 states.[11]

2. The Commission's Past Orders Recognize that Privacy and Data Security Programs Carry Unique Considerations, Focusing on Different Risks.

The Commission's past orders reflect that privacy and data security programs must balance the seriousness of risks against the likelihood of harm, the costs of mitigation, and other compensating controls and factors. ANPR at 16-18. It is unclear why the ANPR combines

[8] Glossary, NAT'L INST. OF STANDARDS AND TECH. (Aug. 2003), https://csrc.nist.gov/glossary/term/information_security

[9] *Cybersecurity Framework 1.0*, NAT'L INST. OF STANDARDS AND TECH. (April 2018), https://www.nist.gov/cyberframework

[10] S*ee* David Brin, *2022 Study: 50% of SMBs Have a Cybersecurity Plan in Place*, UpCity (May 2, 2022) https://upcity.com/experts/small-business-cybersecurity-survey/ (Cybercriminals continue to target the most sensitive sectors like healthcare and schools, forcing them to make incredibly difficult decisions around payments and operations: cybercrime has cost U.S. businesses more than $6.9 billion in 2021).

[11] *See* Nat'l Conf. of State Leg., *Security Breach Notification Laws* (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification- laws.aspx.

privacy and data security despite the past orders focusing on different risks and harms. The Commission's consent orders relating to consumer privacy hinged on companies' harmful or unauthorized use of personal information. The Commission's past settlement orders related to data security have concerned companies' failures to utilize breach mitigation, patch management, data minimization, and other safeguards. Placing both of these into the same record of harm impedes the balancing each discipline seeks to achieve and undermines the progress the Commission has made over the years.

The Commission's past data security cases illustrate the difficulty of grouping data security and privacy.[12] In these past complaints on data security, the Commission has cited various shortcomings by companies that they allege would constitute unfair and deceptive practices. The Commission then lists various security measures that the company must agree to but does not outline or indicate how many are required to become "reasonable" and thus, not unfair or deceptive. To the extent the Commission promulgates rules on this topic, a data security rule should acknowledge that no system can be fully secure all of the time and the Commission should focus on harm when it develops security rules, among other considerations.

Rather than undertaking its own efforts, the FTC should seek to reinforce the existing work in this space. The Commission should look at existing frameworks, such as the widely-adopted NIST Cybersecurity Framework, that are based on a risk-based, flexible, voluntary, and stakeholder-driven approach, and assist companies in implementing the appropriate data security measures. The business community and organizations already work closely with government agencies such as CISA and NIST to ensure effective frameworks for proper data security practices across products and services. For these reasons, data security frameworks allow for a risk-based analysis that invites a comprehensive view of all considerations on a case-by-case basis.

---

[12] Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (May 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover; Press Release, Fed. Trade Comm'n, FTC Requires Zoom to Enhance its Security Practice as Part of Settlement (Nov. 20, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement; Press Release, Fed. Trade Comm'n, Mortgage Analytics Company Settles FTC Allegations It Failed to Ensure Vendor Was Adequately Protecting Consumer Data (Dec. 15, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/12/mortgage-analytics-company-settles-ftc-allegations-it-failed-ensure-vendor-was-adequately-protecting.

Another benefit of this flexible approach is the growing recognition that cybersecurity is a shared responsibility. This awareness has paved the way for public-private partnerships that permit the sharing of timely information about malicious actors' tactics, techniques, and procedures (TTPs) and enabled law enforcement to track cyber-attacks and gangs – including the recovery of stolen funds or ransoms.[13] Another reason for this common understanding is that security incidents are not isolated, they have a cascading effect – harm can promulgate from one network to another – so it is a shared responsibility to improve everyone's cyber posture. For example, the patch to the open-source vulnerability with Log4j was released last December. However, bad actors and state-sponsored advanced persistent threats (APT) continue to exploit organizations that have failed to patch this severe vulnerability,[14] resulting in statements from both the Commission[15] and the CISA[16] urging for immediate patching. The Equifax hack, which compromised the personal information of over 100 million Americans, was largely due to the company's failure to implement a patch to a known open-source vulnerability.[17]

C. The Commission's Rulemaking Authority

The Commission's consumer protection rulemaking authority is limited to what is outlined by Congress. The vehicle for this current rulemaking, the Magnuson-Moss Act, has been previously used by the Commission to target specific, nuanced issues. However, this ANPR's overbreadth conflicts with the relevant statutory requirements and the role preserved for Congress and States.

---

[13] Press Release, U.S. Dep't of Just., Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actos and their Conspirators (July 19, 2022), https://tinyurl.com/yck6s5nn.

[14] Liam Tung, *CISA: Hackers are Still Using Log4Shell to Breach Networks, so Patch Your Systems*, ZDNET (June 24, 2022), https://www.zdnet.com/article/cisa-hackers-are-still-using-log4shell-to-breach-networks-so-patch-your-systems/.

[15] Press Release, Fed. Trade Comm'n, FTC Warns Companies to Remediate Log4j Security Vulnerability (Jan. 4, 2022), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability.

[16] CISA, Alert (AA22-174A): Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems (July 18, 2020), https://www.cisa.gov/uscert/ncas/alerts/aa22-174a.

[17] Alfred Ng, *How the Equifax Hack Happened, and What Still Needs to be Done*, CNET (Sept. 7, 2018), https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

1. The Commission is Acting Outside the Authority Outlined by Congress, Evidenced by Sectoral Legislation and Proposed Federal Privacy Legislation.

The ANPR's vagueness and overbreadth raise concerns about the scope of the agency's authority. Specifically, in "certain extraordinary cases", regulatory agencies, absent clear congressional authorization, cannot issue rules on major questions that affect a large portion of the American economy.[18] This important principle "helps preserve the separation of powers and operates as a vital check on expansive and aggressive assertions of executive authority."[19]

The Commission's current inquiry would extend beyond its express statutory authority – to declare *specific* acts or practices illegal – and prescribes potential trade rules that would affect "large portions of the American economy." The Supreme Court has cautioned against such agency overreach,[20] "When Congress seems slow to solve problems, it may be only natural that those in the Executive Branch might seek to take matters into their own hands. But the Constitution does not authorize agencies to use pen-and-phone regulations as substitutes for laws passed by the people's representatives."[21]

Congress is already exploring options and proposals that would reform the digital economy through comprehensive privacy legislation,[22] including how to account for the essential role that digital advertising plays in creating the open and free Internet we have today. Congress through this process has been able to account for the various costs and considerations – accounting for compliance costs with existing state and privacy regulations, with over 140 countries having privacy laws[23] – when seeking to regulate such major aspects of the economy.

---

[18] *West Virginia v. Env't Prot. Agency,* No. 20-1530 (U.S. June 30, 2022).

[19] *See U.S. Telecom Ass'n v. Fed. Commc'ns Comm'n*, 855 F.3d 381, 417, 419 (D.C. Cir. 2017) (Kavanaugh, J., dissenting from the denial of rehearing en banc); *see* also Jonathan H. Adler, *A "Step Zero" for Delegation*s, Case Legal Studies Research Paper, at 20 (2021), https://ssrn.com/abstract=3686767 (describing how this approach is rooted in two presumptions; a general presumption against the delegation of "major lawmaking authority from Congress to the Executive branch" and a presumption that "Congress intends to make major policy decisions itself.").

[20] *See* Exec. Order. No. 14036, 86 C.F.R. 36987 (2021). Specifically, the Order directs the Commission to use its authority around unfair or deceptive acts or practices to focus on labor, agriculture, health care, and technology.

[21] *West Virginia v. Env't Prot. Agency*, No. 20-1530 (U.S. June 30, 2022) (Gorsuch, J. concurring).

[22] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2021-2022).

[23] *See* Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills*, 169 PRIVACY LAWS & BUS. INT'L REPORT (2021), https://ssrn.com/abstract=3836261.

In these past inquiries, Congress has deemed certain types of information to be so sensitive that its protection warrants trading off other goals like lowering transaction costs or encouraging innovation. These sectoral-specific trade-offs address both behavioral advertising and data security in the context of protected health information, information collected online about children, and consumer information collected by consumer reporting agencies.[24] The Commission should not usurp this function of Congress.

If the Commission wants to ensure its potential trade rule passes judicial scrutiny, then it should focus on specific practices or acts that are unfair or deceptive to consumers by leveraging its existing and robust expertise in enforcement around privacy and data security, as the Commission highlighted in the ANPR. ANPR at 16-18. The Commission should leave the major questions around regulating the digital economy to the legislative process.

2. The ANPR Does Not Meet Its Statutory Requirements and Is Inconsistent with How the Commission Has Used Rulemaking Authority in the Past.

"Administrative agencies are creatures of statute. They accordingly possess only the authority that Congress has provided."[25] Congress has provided the Commission with limited rulemaking authority[26] to adopt trade regulation rules[27] to define specific acts or practices as "unfair"[28] or "deceptive."[29] The Commission must have reason to believe that the alleged "unfair" or "deceptive" acts or practices that are the subject of the proposed rulemaking are

[24] *See* Health Breach Notification Rule, 16 C.F.R. Part 318; Gramm-Leach Bliley Act, Pub. L. No. 106-102, 112 Stat. 1338 (1999); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505.

[25] Nat'l Fed'n of Indep. Bus. v. Dep't of Lab., Occupational Safety and Health Admin., No. 21A244, 2022 WL 120952, at *3 (U.S. Jan. 13, 2022); *see also* Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374 (1986) ("an agency literally has no power to act … unless and until Congress confers power upon it").

[26] 15 U.S.C. § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful").

[27] Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, 15 U.S.C. §§ 2301, *et seq*. (1975).

[28] 15 U.S.C. 45(n) (an act or practice is unfair if it causes or is likely to cause substantial injury, the injury is not reasonably avoidable by consumers, and the injury is not outweighed by benefits to consumers or competition).

[29] 15 U.S.C. § 45(a) (a representation, omission or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers).

prevalent.[30] Prevalence can be established by cease-and-desist orders against specific past practices or any other information that indicates widespread patterns of unfair or deceptive acts.[31] And the ANPR, amongst other requirements, must "contain a brief description of the area of inquiry under consideration, the objective which the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission."[32]

The current ANPR consists of 95 wide-ranging questions and, as Commissioner Phillips noted in his dissent, "provides no notice whatsoever of the scope and parameters of what rule or rules might follow; thereby, undermining the public input and congressional notification processes"[33] The Commission is required to establish a record indicating the prevalence of a specific "unfair" or "deceptive" act or practice. The Commission has adhered to this specificity with past ANPRs that have narrowly tailored to discrete issues like deceptive and unfair earnings[34] or clothing washing labels.[35] The Commission's ability to establish prevalence is the strongest where the agency has previously engaged in fact-finding through fact-intensive investigations, comprehensive information gathering, and administrative adjudication.

However, the current ANPR seeks to touch upon concerns that the Commission itself has not raised in past settlement or consent orders relating to data privacy and security – such as "psychological harms" or creating per se rules around certain types of data. ANPR at 26, 37. The Commission has not identified any court decisions or administrative orders indicating such harms' prevalence. Rather, the Commission only cites consumer-generated complaints and media articles that touch upon a wide range of practices involving data, not necessarily related to specific concerns about the specific practices contemplated for rulemaking. ANPR at 22, 26.

A sweeping prohibition of a practice is certainly inappropriate when, as here, the ANPR provides merely anecdotal evidence about only bad actors or speculates about some possible

---

[30] 15 U.S.C. § 57a(b)(3).
[31] 15 U.S.C. § 57a(b)(3)(A)-(B).
[32] 16 C.F.R. § 1.10.
[33] *See* Office of Commissioner Noah Joshua Phillips, *Dissenting Statement of Commissioner Phillips,* FED. TRADE COMM'N (Aug. 11, 2022) ["Phillips Dissent"].
[34] *See* Deceptive or Unfair Earnings Claims, 87 Fed. Reg. 13951 (proposed Mar. 11, 2022), https://www.federalregister.gov/documents/2022/03/11/2022-04679/deceptive-or-unfair-earnings-claims.
[35] *See* Trade Regulation Rule on Care Labeling of Textile Wearing Apparel and Certain Piece Goods, 85 Fed. Reg. 44485 (proposed July 23, 2020), https://www.federalregister.gov/documents/2020/07/23/2020-13919/trade-regulation-rule-on-care-labeling-of-textile-wearing-apparel-and-certain-piece-goods.

harms amongst a sea of pro-competitive and consumer benefits. Employing an *ultra vires* legislative rulemaking for the entire Internet marketplace would not be sensible when a clearly authorized, routinized means of case-by-case review, which benefits from the continued evolution of economic and industrial learning, is the more tested, sure, and tailored approach if illegal conduct were discovered.

3. The ANPR Suggests New Limitations of Ownership that Go Beyond the Commission's Rulemaking Authority, Which Does Not Extend to Unfair Methods Of Competition.

The ANPR explores new limitations of company ownership that would extend the Agency's authority beyond what Congress has authorized and the its own longstanding view of this narrow authority. ANPR at 31.

Congress in Magnuson-Moss, expressly limited the Commission's authority to adopt trade regulation rules implementing only the unfair or deceptive clause of Section 5. Congress declined to extend the Commission's authority to include unfair methods of competition. In the years since its passing, Congress has directed the FTC to use informal notice and comment rulemaking, through statutes that provide the agency with detailed guidance on rulemaking topics and goals and that specifically provide exemptions from the procedures for Magnuson-Moss rulemaking. For example, such specific instruction has been given for the Telephone Disclosure and Dispute Resolution Act of 1992, the Children's Online Privacy Protection Act of 1998, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. In these instances, Congress has made a clear grant of authority to the FTC, with detailed guidance on rulemaking topics and goals. If Magnuson-Moss was not intended to outline the scope of the FTC's rulemaking authority, these Congressionally-permitted exceptions would not 6be necessary. And, notably, no such Congressional directive has been given to the FTC to engage in unfair methods of competition rulemaking.

And the Commission's prior reticence to engage in antitrust rulemaking is instructive on its ability to do so. In the recent *AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n*, the Supreme Court stated, "In construing § 13(b), it is helpful to understand how the Commission's authority (and its interpretation of that authority) has evolved over time."[36] An agency's longstanding view that it lacks the authority to take a certain action is a "rather telling" clue that the agency's

[36] 141 S. Ct. 1341, 1346-47 (2021).

newfound claim to such authority is incorrect.[37]

The Commission should not commence a rulemaking that is not within its authority to conduct.

4. The Commission Must Rely On The Factors Outlined In Section 5 Of The FTC Act When Balancing The Costs And Benefits Of New Rules.

Consumers benefit when the Commission engages in thorough, objective assessments that rely on evidence-based analysis, grounded in principles of consumer protection, support for competition, and cost-benefit considerations. CCIA agrees that specific bad practices must be dealt with, but the Commission should continue to rely on the existing framework for unfairness outlined in Section 5 of the FTC Act for this analysis. Otherwise, there is a serious risk that any broad trade rule would be too prescriptive, ultimately inhibiting innovation and harming consumers and competition in the process.

The Commission in Question 24 invites all comments "on the relative cost and benefits of any current practice," including "which variables or outcomes are salient but hard to quantify as a material cost and benefits?" ANPR at 29. The Commission cites no reason for its departure from its long-established practice of adhering to what Congress outlined in the FTC Act when granting the Commission authority to investigate particular issues affecting commerce.

Under Section 5 of the FTC Act, the Commission can declare an act or practice "unfair" only if it 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."[38] The Commission is required to balance consumer welfare tradeoffs.[39] While the Commission may want to explore other factors, it should remain cautious of repeating past

[37] *Loving v. IRS*, 742 F.3d 1013, 1021 (D.C. Cir. 2014) (Kavanaugh, J.) ("In light of the text, history, structure, and context of the statute, it becomes apparent that the IRS never before adopted its current interpretation for a reason: It is incorrect.").

[38] 15 U.S.C. § 45(n).

[39] *See* Michael R. Baye & Joshua D. Wright, *How to Economize Consumer Protection*, ANTITRUST SOURCE (Feb. 2018), https://ssrn.com/abstract=3137122 ("… economics can be used in consumer protection matters to help prove or disprove a claim that a business practice adversely impacted consumer").

mistakes that led to instances of overreach.[40]

The parameters of the unfairness standard have been explained and discussed in the context of consumer privacy by the Commission and other experts.[41] But the breadth of this ANPR makes it difficult, if not impossible, to meaningfully contribute to the cost-benefit analysis discussion. As Commissioner Phillips notes, "the Commission would be more likely to receive helpful data if it asked commenters for the costs and benefits of some defined kind of conduct, or a particular rule to regulate it."[42] Furthermore, the questions only reference potential harms around targeted advertising, failing to mention any potential consumer benefits and pro-competitive improvements that may arise from such practices.

The Commission must also demonstrate that specific substantial injury is not reasonably avoidable. The Commission can look at alternatives such as exploring whether an opt-out mechanism would suffice. Lastly, the Commission must also weigh the countervailing benefits against the specific harms. However, the Commission proposes to prohibit certain companies from engaging in targeted advertising, without citing any substantial harms. ANPR at 31. This not only misrepresents the nature and structure of how these services operate but underestimates the overwhelming benefits they have produced, including supporting and funding the current Internet ecosystem.

5. The Commission Has Stronger Alternatives to This Scopeless Inquiry, Including Addressing Specific Issues That Are Ripe for Rulemaking.

The Commission should not usurp this function of Congress, particularly when its longstanding authority to investigate potentially unlawful activity on a case-by-case basis remains available. This would continue to leverage the Commissioners' and agency's expertise with privacy and data security issues for the benefit of consumers and competition.

Instead of embarking on a scopeless rulemaking, to supplement its robust case-by-case

---

[40] *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM'N (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-itsrise-fall-and-resurrection; *The FTC as National Nanny,* WASH. POST (Mar. 1, 1978), at A22.
[41] Tad Lipsky, et al, *The Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century: Consumer Privacy, Comment of the Global Antitrust Institute, Antonin Scalia Law School, George Mason University,* THE GLOBAL ANTITRUST INSTITUTE (Feb. 19, 2019), https://gai.gmu.edu/wp-content/uploads/sites/27/2019/02/FTC-consumer-privacy.SSRN-.pdf.
[42] Phillips Dissent, at 4.

rulemaking authority, the Commission can issue guidance and policy statements and can serve as an advisory agency to Congress in its efforts to enact comprehensive federal privacy legislation. The Commission could identify sensitive information and require that firms enact plans to mitigate the risk of harm from using that type of information, enabling firms themselves to assess tradeoffs. This risk-based approach would increase transparency to consumers and create consumers' reasonable expectations about transacting with the firm. In particular, the Commission can look at NIST's privacy framework and core principles that further reflect the importance of this risk-based approach, permitting companies to flexibly tailor their data practices to respond to specific scenarios.[43]

The Commission should also host workshops around the market and consumer-driven innovations that advance both security and privacy. For example, in the digital advertising market, businesses have invested in technologies that reduce the reliance on third-party tracking through cookies and other personal identifiers. Such initiatives include Mozilla and Meta's joint "interoperable private attribution" proposal,[44] which could improve cross-device or cross-browser attribution in a privacy-preserving way.

The Commission should also host hearings tailored to the various regulatory schemes created by states and other federal agencies around data security and privacy. This would provide a useful platform to learn about successes and unintended costs with these approaches, further helping the Commission shape a narrower rule. In particular, the Food and Drugs Amendments of 2022, which are tailored to the security of medical devices, offers a promising sector-by-sector approach to risk-based cybersecurity regulation.[45]

Lastly, the Commission could help businesses reduce and better manage cybersecurity risks by providing guidance on a data security baseline for future enforcement. This risk-based analysis, should adopt a comprehensive view of all considerations on a case-by-case basis. This would balance the crucial flexibility needed for data security and provide predictability for future

---

[43] *Privacy Framework*, NAT'L INST. OF STANDARDS AND TECH. (Jan. 2020), https://www.nist.gov/privacy-framework/privacy-framework.

[44] Martin Thomson, *Privacy Preserving Attribution for Advertising*, MOZILLA (Feb. 8, 2022), https://blog.mozilla.org/en/mozilla/news/privacy-preserving-attribution-for-advertising/.

[45] *See* Jim Dempsey, *Medical Device Security Offers Proving Ground for Cybersecurity Action*, LAWFARE (June 9, 2022), https://www.lawfareblog.com/medical-device-security-offers-proving-ground-cybersecurity-action.

enforcement. This would remedy the shortcomings raised by the court in the *LabMD v. FTC,* where the court held that the agency's order mandating a company to rebuild its entire data security program was held overly broad and failed to enjoin a specific act or practice.[46] The Commission can leverage its past incremental record of enforcement actions, statements, and reports to articulate the considerations for this balancing test and outline what could constitute "reasonable" data security measures. The Commission can also provide a policy statement on privacy and data, which, for example, could outline how the principles in the statements on "Unfairness"[47] and "Deception"[48] could apply in these contexts.

D. The Commission Has Sufficient Enforcement Authority to Address Practices Meeting the Section 5 Standard of Unfairness.

The Commission's authority to investigate and address unfair and deceptive acts is plenary, as the ANPR itself demonstrates in identifying more than two dozen agency proceedings and federal lawsuits against practices that infringe or ignore consumers' privacy. ANPR at 16-19. These cases have created a set of jurisprudence that establishes, for both businesses and consumers, the rules of the road for issues such as data collection, sale, and transfer, surreptitious installation of "stalkerware", and failure to adhere to published privacy policies. Conduct related to sensitive consumer data, if it meets the three-part test of Section 5, can be and has been stopped.

In the privacy context, the most important aim of enforcement is securing a cessation of injurious conduct with a commitment not to repeat it. Sections 5 of the FTC Act authorize the FTC to pursue those results. And the Commission's enforcement activity of the last few decades amply shows that it has the statutory tools, expertise, and resources to protect consumers from being deceived or disadvantaged in the way that their data is collected, stored, shared, and used. The Commission's enforcement authority has been effective, enabling consumer protections to evolve under this framework without inhibiting innovation.

---

[46] *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221 (11th Cir. 2018).

[47] *FTC Policy Statement on Unfairness,* FED. TRADE COMM'N (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.

[48] *FTC Policy Statement on Deception*, FED. TRADE COMM'N (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf

E. The Commission Must Adhere to the Procedural Requirements When Considering to Regulate Privacy

The Commission faces numerous substantive and procedural obstacles in considering broad rulemaking on privacy. In addition to the challenges as described by Commission Slaughter, the Commission would need to adhere to extensive requirements on transparency, hearings, designation of issues, and encouraging staff participation, where the expertise rests.[49]

1. The Commission Should Continue to Place a High Priority on Transparency.

The online consumer marketplace is growing at an exponential rate, with mobile technologies providing enormous value to both businesses and consumers.[50] Lack of attention to transparency could lead to an erosion of trust in the mobile marketplace, which could be detrimental to both consumers and the industry.[51] The ANPR appropriately raises transparency as a key component of privacy protection. ANPR at 20-21, 38-40.

Transparency is a core tenet of all good privacy practices, as it is important for consumers to know what information is being collected and how that information is used when they are online. For example, as Commissioner Wilson notes in her speech at the Future of Privacy Forum, "privacy legislation should embrace the notion that transparency empowers individuals to make informed choices. Consumers need clarity regarding how their data is collected, used, and shared."[52] David Vladeck, the former Director of the FTC's Consumer Protection Bureau also explains how it is vital to "promote transparency of privacy practices" and enable

---

[49] Any broad rulemaking needs to satisfy either the Unfair or Deceptive standard, identify prevalence of that specific act or practice, and not expand the Commission's authority beyond what is granted in Section 5. *See* Office of Commissioner Rebecca Kelly Slaughter, *Statement of Commissioner Rebecca Kelly Slaughter,* Federal Trade Commission, Aug. 11, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/RKS%20ANPR%20Statement%2008112022.pdf.

[50] FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

[51] *See* Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Technology and the Law, 112th Cong. (2011).

[52] FTC Comm'r Christine S. Wilson, *A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Legislation,* Remarks at the Future of Privacy Forum (Feb. 6, 2020), at 13, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_spee ch_02-06-2020.pdf.

"consumers to exercise meaningful choice.[53] Consumers need to understand how the information they share will be used, so that they can make informed decisions about whether to share it in the first place.[54]

Over the past two decades, the Commission has developed multiple reports examining the state of online privacy and the efficacy of industry self-regulation as well. From its report to Congress on privacy in 2000[55] to its 2012 Privacy Report[56] to more recent reports about specific industries, such as the data broker industry and the broadband industry, the FTC emphasized the importance of transparency in data practices.[57] For example, in its 2012 report, the Commission expressed support for clear disclosures accompanying "just-in-time" choices. In its report on the data broker industry, the FTC called for greater transparency and accountability. And in its most recent report on the broadband industry, the FTC called for clearer disclosures of practices and choices.

In addition to giving consumers actionable information, transparency also allows the FTC to hold companies accountable. The Commission has already promoted transparency by bringing data privacy cases under Section 5 of the FTC Act. [58] As Commissioner Slaughter has noted, the FTC "has been nimble and aggressive in its attempts to use" its Section 5 unfairness and deception authorities "to police today's technology-driven marketplace with many successes."[59] For example, the Commission has brought actions for sharing health information of users after

---

[53] David C. Vladeck, *Promoting Consumer Privacy: Accountability and Transparency in the Modern World*, Remarks of David C. Vladeck, former Director, FTC Bureau of Consumer Protection, N.Y. UNIV. (Oct. 2, 2009), at 13.

[54] *See id.*

[55] FED. TRADE COMM'N, *Privacy Online: Fair Information Practices In The Electronic Marketplace*, Report to Congress (May 2000).

[56] FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change*, Recommendations for Businesses and Policymakers (Mar. 2012).

[57] *See id.*

[58] 15 U.S.C. § 45.

[59] *See* Tr. of FTC Hr'g, *The FTC's Approach to Consumer Privacy* (Apr. 10, 2019), at 134, https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf.

promising that such information would be kept private;[60] retroactive application of material privacy policy changes to personal information that businesses previously collected from users;[61] deceiving consumers by telling them they could keep their information on private, and then repeatedly allowing it to be shared;[62] failing to disclose adequately the scope of consumers' personal information collected;[63] collecting personal information from their mobile device address books without their knowledge and consent.[64]

The list above is just a small sample of the FTC's enforcement work in promoting transparency in the world of data privacy.[65] For more than two decades, the Commission has been the nation's leading consumer privacy enforcement authority, and it should continue to use its Section 5 authority to promote transparency in the online marketplace. Transparency is the backbone of privacy protection, and the CCIA is eager to see the FTC continue its great work in allowing consumers to feel confident that they have control over their personal data, which will promote trust and participation in the digital economy.

2. Behavioral Advertising Continues to Provide Core, If Not Irreplaceable, Value to Consumers, Publishers, and Advertisers.

---

[60] *See* Press Release, Fed. Trade Comm'n, Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about.

[61] *See*, *e.g.*, Compl., *In the Matter of Gateway Learning Corp*., FTC. File No. 042-3047 (Sept. 10, 2004), https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf.

[62] *See* Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises.

[63] Compl*., In the Matter of Sears Holdings Mgmt. Corp.,* FTC File No. 082-3099 (Sept. 9, 2009), http://www.ftc.gov /os/caselist/0823099/index.shtm.

[64] *See* Press Release, Fed. Trade Comm'n, Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived-consumers-improperly-collected-personal.

[65] *See also*, *e.g.*, Compl., *In the Matter of Turn Inc*., FTC File No. 152-3099 (Apr. 6, 2017), https://www.ftc.gov/system/files/documents/cases/152_3099_c4612_turn_complaint.pdf (Respondent deceptively tracked consumers online and through their mobile applications for advertising purposes even after consumers took steps to opt out of such tracking); Compl., *In the Matter of ScanScout, Inc*., FTC File No. 102-3185 (Dec. 14, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutcmpt.pdf (Respondent deceptively used flash cookies to collect for advertising purposes the data of consumers who changed their web browser settings to block cookies).

Digital advertising generates hundreds of billions in revenue per year in the United States. Zenith Media estimates that nearly $183 billion was spent on digital advertising in 2021,[66] accounting for nearly 64% of all major media advertising spending in the U.S.[67] Online marketing and advertising have become a crucial mainstay of the U.S. economy. It is thus evident that online marketing and advertising has become a crucial mainstay of the U.S. economy.

Ads fuel the Internet, which "is advantageous for both advertisers and consumers."[68] Behavioral advertising, as compared to other forms of advertising, offers advertisers an efficient method of precisely targeting a valuable demographic.[69] It is commonplace in the digital space because it is useful to advertisers, publishers, and consumers. Customizing ad displays helps advertisers reach interested consumers at lower costs and increases the value of publishers' online advertising "real estate" associated with their digital content. In addition, personalization increases the odds that, when consumers see advertising, those ads pertain to products and services that are actually meaningful to them.

Rather than presenting users with ads for products for which they have no use, behavioral advertising enables firms to display the items that are far more relevant to the consumer. And that consumer, rather than being deluged with irrelevant ads, will see a sensible array of products and services more likely of interest to them. In short, behavioral advertising improves efficiency and increases value. For these reasons, "the technology also helps small businesses compete, even when their customers would ordinarily reach through other advertising outlets."[70] The benefits of behavioral advertising are therefore plainly evident, which shows that the "countervailing benefits" element of Section 5 cautions against Commission action.

---

[66] Brad Adgate, *Agencies Agree; 2021 Was a Record Year for Ad Spending, with More Growth Expected in 2022*, FORBES (Dec. 8, 2021), https://www.forbes.com/sites/bradadgate/2021/12/08/agencies-agree-2021-was-a-record-year-for-ad-spending-with-more-growth-expected-in-2022/?sh=4a32828d7bc6.

[67] *Id*.

[68] Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA HIGH TECH. L.J. 3, 31 (2012), http://digitalcommons.law.scu.edu/chtlj/vol27/iss1/2.

[69] Andrew Hotaling, *Protecting Personally Identifying Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMM LAW CONSPECTUS: J. OF COMMC'NS L. & TECH. POLICY 529, 533-38 (2008), https://scholarship.law.edu/commlaw/vol16/iss2/10.

[70] Berger, *Balancing Consumer Privacy,* at 31.

Concerns about behavioral advertising, *see* ANPR at 3, can obscure the pro-consumer and pro-ecosystem effects created by this highly evolved method of consumer outreach. To presume that behavioral advertising is an inherently harmful practice, and adopt rules built on that presumption, threatens to upend consumer welfare and online business models. [71]

The Commission recognized as recently as 2020 that behavioral advertising benefits consumers.[72] According to the FTC Bureau of Economics, the value of behavioral advertising takes myriad forms:

- "[T]argeting benefits the consumer because it effectively reduces their search costs." *Id*. at 5.
- "Search cost reduction [sic] and improved match quality" creates "greater price competition between firms in equilibrium." *Id*. at 6.
- "Precise targeting … could lower marketing costs for firms by reducing wastage of ads served to disinterested consumers vis-à-vis the untargeted alternative." *Id*. at 6 (internal citation omitted).
- "[T]he targeted ad-supported business model essentially allows individual consumers to monetize their personal data in exchange for valuable digital goods and services, financed by revenues from targeted ads." *Id*. at 11.

The Bureau went on to caution that placing onerous restrictions on targeted ads would upend the online commercial model, creating a revenue void in which consumers would suffer an "income effect" by having to pay for online services currently available for free, like free search. *Id*. at 11. This income effect would particularly harm low-income consumers. *Id*. The Commission has, in fact, recognized the risks of hyper-regulation with regard to behavioral advertising for more than a decade.[73] These analyses and policy statements militate against a

---

[71] Behavioral advertising saves time and increases value for both sides of the online marketplace. *See* Comments of the CCIA, *Petition of Accountable Tech for Rulemaking to Prohibit Surveillance Advertising*, File R2007005 (Jan. 26, 2022).

[72] YAN LAU, FED. TRADE COMM'N, *A BRIEF PRIMER ON THE ECONOMICS OF TARGETED ADVERTISING* (Jan. 2020), https://www.ftc.gov/reports/brief-primer-economics-targeted-advertising.

[73] FED. TRADE COMM'N, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, at 9-10 (Feb. 2009), ("Online behavioral advertising may provide valuable benefits to consumers in the form of free content, personalization that many consumers appear to value, and a potential reduction in unwanted advertising."); Vladeck, *Promoting Consumer Privacy: Accountability and Transparency in the Modern World*, ("[I]f we were to ban behavioral advertising altogether, consumers would not have access to much of the free online content they have come to expect.").

finding that behavioral advertising satisfies the harm element of Section 5.

Behavioral advertising is not "impossible for any one person to avoid." ANPR at 3. The concerns that consumers recently have raised about this practice were addressed via swift industry response. Many platforms began phasing out the use of cookies in 2019, despite the financial consequences that might have hit their advertising revenues.[74] According to one study, "almost 40% of marketers have already limited their reliance on consumer tracking by third-party cookies."[75] Industry groups and individual companies offer robust opt-outs.[76] Consumers are able to avoid behavioral advertising in large part, which again goes to the question of whether the Section 5 harm element is satisfied.

3. Consent Remains the Cornerstone of Good Privacy Policy.

The ANPR asks, "to what extent does current law prohibit commercial surveillance practices, irrespective of whether consumers consent to them?" ANPR at 37.

Meaningful consent for consumers and strong controls can provide consumers with strong tools to ensure their privacy expectations are met. A per se rule that would overrule consent challenges the existing relationships between consumers and businesses and what other jurisdictions have done regarding this sensitive issue. For example, some jurisdictions have created opt-out rights for data processing for the sale to third parties, cross-platform targeted advertising, and profiling in furtherance of decisions with legal or similarly significant effects. For data processing that presents particular risks, lawmakers have considered requirements that controllers obtain affirmative consent before the collection of sensitive data. The Commission should look at these carefully negotiated proposals to ensure any rule aligns with the reasonable expectations of consumers.

Any future rulemaking should take a flexible approach to what qualifies as consent in order to facilitate customer experiences across a range of devices and services. It should not

---

[74] Alexander Bleier, *On the Viability of Contextual Advertising as a Privacy-Preserving Alternative to Behavioral Advertising on the Web,* FRANKFURT SCH. OF FIN. & MGMT,, at 2, 5 (Dec. 7, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3980001 (Apple, Google, and Mozilla have discontinued cookies within their browsers).

[75] Bleier, *Viability of Contextual Advertising*, at 5.

[76] *See*, e.g., Turn off personalized ads, Google Ads Help (last accessed Nov. 11, 2022), https://support.google.com/ads/answer/2662922?hl=en.

prescribe required forms of consent. The scope of permitted consent should be broad enough to cover a range of data types and data uses. They should not preclude a company from offering customers the option to provide a one-stop shop for providing consent for how their data is used across experiences. For instance, in setting up consent permissions for a child, the rules should not prevent a parent from having the option to provide a single consent for different types of personal data or for processing data for different experiences such as music and video. And consent should not be defined in a way that limits a company to collecting or processing data only for functions or programs that exist at the time of the consent. Customers benefit from the speedy launch of new experiences and features, which they would be denied if the company had to restart the consent process for every innovation.

4. Pro-Consumer Data Minimization and Purpose Limitation Practices Are Already Widely Used.

The Commission's questions about data minimization practices, ANPR at 32-33, are an important inquiry. The Commission has previously acknowledged that data collected to provide one service can be used to create huge benefits to consumers and society in another context. In particular, big data could accelerate advances in medicine, education, health, and transportation – in many instances without using consumers' personally identifiable information.[77] The Commission has also recognized the utility of large data sets in identifying and reducing discriminatory harm and offering new potential solutions to discriminatory harms.

In the past, Commissioner Slaughter has raised concerns around data minimization[78] and so has the Commission with its recent enforcement actions.[79] However, any proposed generalized data minimization requirement must adhere to the requirements under Section 5 of the FTC Act. The Commission, when conducting its analysis of the benefits and harms of such

[77] FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[78] FTC Comm'r Rebecca Slaughter, *Wait But Why? Rethinking Assumptions About Surveillance Advertising*, Remarks at the IAPP Privacy Security Risk Closing Keynote (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597998/iapp_psr_2021_102221_final2.pdf.

[79] Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (May 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

practices, can look at how the industry and consumer preference have paved the way for innovation around security and privacy.

Privacy is best secured through anonymization, a goal that might never fully be reached, or, if reached, would strip data of all utility. Privacy-enhancing technologies (PETs), most notably differential privacy (DP), are a key tool to minimize data processing. Rather than attempt data de-identification, which is increasingly difficult and susceptible to reverse engineering, PETs offer an array of tools to enable data minimization. PETs have significantly lowered the baseline of risk associated with handing over one's data and made the incremental increases of risk much smaller. PETs have introduced machine learning (artificial intelligence) into data privacy, which "has the power to reveal information that would not be obvious to a human evaluating a dataset unassisted."[80]

Apple and Google already use DP in their respective mobile operating systems. Apple built DP into iOS 10 for all data collection and uses it for improving pre-installed applications like Notes and the keyboard.[81] Google, credited with developing federated learning, uses it for word recommendations on the Android keyboard.[82] In addition, IBM and Uber have released open-sourced libraries for experimenting with various DP applications.[83]

The Commission should also seek to account for the specific tradeoffs between privacy and security with any proposed trade rule, especially given how adversely impactful some technical mandates like rushed interoperability can be.[84]

The Commission has recognized the importance of flexibility in permitting innovative new uses of data that benefit consumers and should continue to do so with Data Minimization. The Commission could look at other standards adopted by states such as Virginia that promote

---

[80] Andrea Scripa Els, *Artificial Intelligence as a Digital Privacy Protector*, 31 HARV. J.L. & TECH. 217, 218 (2017).

[81] Andrea Scrips Els, at 221; Fang Liu, Ph.D., *A Statistical Overview on Data Privacy*, 34 Notre Dame J.L. Ethics & Pub. Pol'y 477, 478 (2020).

[82] *Id*.

[83] Fang Lui, *A Statistical Overview on Data Privacy*, at 486.

[84] *See* Mikołaj Barczentewicz, *Privacy and Security Implications of Regulation of Digital Services in the EU and in the US*, TTLF Working Paper No. 84, STANFORD-VIENNA TRANSATLANTIC TECH. L. FORUM (2022), http://law.stanford.edu/wp-content/uploads/2022/01/TTLF-WP-84_Barczentewicz.pdf ("A crude interoperability mandate could make it much more difficult for service providers to keep up with the fast-evolving threat landscape… Even today, email continues to be a source of security concerns due to its prioritization of interoperability").

innovation through its reasonably necessary standard.[85] This would limit enforcement to data collection and uses that are unambiguously outside the bounds of this standard.

5. Concerns About Automated Decision-Making Are Insufficient Ground on Which to Base New Rules Absent Clear Scope, Demonstrable Harm, and Delimited Breadth.

The ANPR does not attempt to define the scope of its inquiry into automated decision-making ("ADM"), which is not a universally defined term and could encompass a wide range of technology from spreadsheets to autonomous vehicles. Again, the Commission must cite and find specific harm, determine if any alternatives could address it, and whether the countervailing benefits outweigh the alleged harm. An overly broad regulation of ADM technology may stymie the use of socially beneficial, low-risk, and widely accepted tools, to the significant detriment of both consumers and businesses.

However, this is not what the ANPR is seeking to do. ANPR at 34-36. Rather, as noted by Commissioner Phillips, the ANPR seeks to unilaterally declare a wide range of technologies unfair.[86] This diverges from the Commission's past narrowly tailored workshops and enforcement actions on artificial intelligence and related technologies, where did not indicate that the use of such technologies or practices to be "unfair."[87] The ANPR creates further confusion about the scope of this possible blanket ban by failing to distinguish between automated decision-making, algorithmic decision-making, and whether there should be a threshold requirement for human input.

The ANPR is silent on the various pro-competitive efficiencies and consumer benefits that ADM has created in countless sectors.[88] The Commission should not bypass this statutory

[85] *See* Virginia Consumer Data Protection Act, S.B. 1392 § 59.1-574. ("A controller limits the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer").

[86] Phillips Dissent, at 5 ("For example, while the Commission has explored facial recognition and automated decision-making in workshops and reports, it has never found that the use of facial recognition technology or automated decision-making themselves to be unfair").

[87] *See* Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FED. TRADE COMM'N (April 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai

[88] Arash Aghlara, *Decision Automation Benefit*, FLEXRULE (Sept. 2020), https://www.flexrule.com/archives/decision-automation-benefits/.

requirement to consider benefits when exploring rules to regulate automated decision-making. This neglects to account for the benefits that automated to semi-automated technologies have created for various generic and niche entrepreneurs. The Commission should also address the costs with creating and imposing possible thresholds across various industries, and upon a smaller and medium-sized business that cannot afford to employ dozens to hundreds of human reviewers.

Any rules concerning automated decision-making should focus on securing protections for consumers with respect to fully automated decisions that may have legal or similarly significant effects. The rules should not create unnecessary restrictions for low-risk systems and tools that support ordinary business operations and transactions.

Even where automated decision-making produces legal or similarly significant effects, it may still be highly beneficial to consumers – and if turned off, creates the risk of potential harm. For example, a healthcare system that uses an individual's address to select the closest ambulance dispatch location; a bank that uses income or account balance to assess available credit; or fraud detection and related activities in making financial or insurance decisions. Accordingly, to the extent certain uses of ADM are restricted, there should be appropriate carve-outs for any processing relating to fraud prevention, anti-money laundering processes, screening, or for another type of security or compliance activities. Failure to do so would, for example, enable bad actors to avoid or opt-out of automated processes that detect and block their fraudulent activities, and limit companies' ability to protect customers' privacy and security.

6. Attempts to Address Discrimination Via Privacy Regulation Are Misplaced.

The ANPR asks a series of questions on algorithmic discrimination. To the extent that the Commission has concerns about how such technology might be misused to discriminate against a consumer or class of consumers, ANPR at 8, the Commission should not seek to address these concerns through rulemaking.

To the extent that the Commission has concerns about how automated decision-making might be misused to discriminate against a consumer or class of consumers, ANPR at 8, existing civil rights law is the more apt and better-developed legal framework for such violations. Were two, entirely separate bodies of federal law – civil rights law and privacy law – to become simultaneously enforceable, the legal system would be beset with confusion and duplicative legal

claims.

If in fact, the Commission's inquiry reveals evidence that consumers are being harmed via undisclosed online practices, any resultant Commission action should focus on the deception inherent in such conduct. If a consumer was kept in ignorance of requested information or gave information to a degree or for a purpose of which they were unaware, that harm may fall within the Commission's Section 5 authority to address deceptive practices. Grafting concepts better suited to enforcement of civil rights laws, like the "protected class" construct, would take the Commission down a path that other agencies equipped with the proper authority are best positioned to address.

7. Any Consideration of Biometrics Should Be Tied to Data that Directly Ties to a Unique Individual in a Manner that Could Cause Cognizable Harm.

The term "biometrics" refers to the unique and distinguishable biological characteristics (both physiological and behavioral)[89] of an individual.[90] Physiological characteristics may include hand geometry, palm and vein patterns, fingerprints, DNA, face geometry, and retina, iris, or ear features.[91] Behavioral characteristics are measurable patterns of human behavior such as typing rhythm, gait, and voice patterns.[92] In the public sector, federal security and law enforcement agencies collect and use biometrics for border control and cybersecurity.[93] In the private sector, biometrics are an optional tool that consumers can use to make devices and online experiences more streamlined – they can choose to use their own biometric data to unlock smartphones, log into mobile apps, and complete financial transactions.[94] Biometric data thus has

[89] *FAQ - Biometrics,* 360 BIOMETRICS, http://www.360biometrics.com/faq/biometrics.php (last visited Oct. 3, 2022).
[90] *See Definition: Biometric Verification,* TECHTARGET, https://www.techtarget.com/searchsecurity/definition/biometric-verification (last updated July 2021).
[91] Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information,* 66 U. KAN. L. REV. 637, 671 (2018).
[92] *See id.* at 640.
[93] *See* Tom Simonite, *Face Recognition Is Being Banned—but It's Still Everywhere*, WIRED (Dec. 22, 2021), https://www.wired.com/story/face-recognition-banned-but-everywhere/ (CBP has implemented face recognition gates for incoming travelers at almost 200 airports).
[94] Chloe Stepney, A*ctual Harm Means It Is Too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law*, 40 LOY. L.A. ENT. L. REV. 51, 53 (2020); *See also* Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric*

significant benefits in enhancing data and device security, preventing fraud, and assisting in public safety efforts.

Biometric data that identifies unique individuals and exposes them to loss or injury warrants protection. The scope in which biometric data can be used to identify a person must be limited to preserve trust in the digital marketplace.

Consumers should be given the appropriate ability to consent, and the commission has the ability to pursue companies that engage in unfair practices. The Commission has the power to bring an enforcement action against companies who have engaged in unfair or deceptive practices like non-compliance with privacy policies or the use of facial recognition technologies without proper notification.[95] For example, the FTC enforced an action against the developer of a photo app in 2017 when it deceived consumers about its use of facial recognition technology and its retention of the content of users who deactivated their accounts.[96] As part of the settlement with the FTC, the company must obtain consumers' express consent before using biometric information it collected from them.[97] That case is a perfect example of how the Commission already uses its enforcement powers to regulate data practices without going through the steps of promulgating a new rule.

But, to the extent the Commission promulgates rules on this topic, they should require affirmative and informed consent (including written, verbal, or other clear, unambiguous acts) for collection of biometric data. These consent rules should also reflect the following parameters:

- Require consent only when the controller stores the data, and not when collection is for an ephemeral use and then immediately purged (for example, to check if someone is enrolled in a service) or when the data is solely stored on user devices. Consent should be required only at the stage where the consumer enrolls in a service – the consumer should not then be required to consent every time the collected biometric identifier is used to perform the service, such as to authenticate identity.

Information, BUS. L. TODAY (May 2016) (MasterCard announced in 2016 that it would accept "selfies" in lieu of passwords for cardholders to sign into their accounts).

[95] Kelly A. Wong, *The Face-ID Revolution: The Balance Between Pro-Market and Pro-Consumer Biometric Privacy Regulation*, 20 J. HIGH TECH. L. 229, 237 (Jan. 2020).

[96] Press Release, Fed. Trade Comm'n, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology.

[97] *See id.*

- Avoid consent requirements that would result in eliminating products and services that generate substantial consumer benefit, with minimal risk of unfair or deceptive consequences. For instance, consumers routinely use online photo album features that automatically sort contacts based on facial geometry. A broad consent rule would wipe out this feature since it would be impossible to obtain consent from all of these contacts.

- Exempt consent for security and emergency situations. For instance, stores should have the ability to screen for known criminals or shoplifters, who would not otherwise consent. Facial recognition technology should also be permitted to screen for a missing person, who is not available to provide consent.

- Scope of covered biometrics: The scope of regulations should be limited to biometric identifiers, i.e., data generated by automatic measurements of an individual's biological characteristics that is used to identify a specific individual. It should not cover merely the collection of data from which biometric identifiers may be pulled, such as a physical or digital photograph, a video or audio recording or data generated therefrom unless such data is generated to identify a specific person

These recommendations align with the values of our organization as well, as CCIA emphasizes the importance of strong data privacy protections while maintaining open markets and full, fair, and open competition.

8. Rules That Focus on Technological Prescription Rather Than Policy Principles Risk Becoming Obsolete.

Any consideration of privacy guidelines should involve an express consideration of how they will affect competition and innovation.[98] As CCIA has previously mentioned to the Commission, adopting a prescriptive approach may create a framework that is inapplicable to later technological developments.[99] For example, in public remarks to the FTC at the September 8, 2022 public forum about commercial surveillance, CCIA emphasized that there is a risk of obsolescence when rules embrace prescription over normative guidance.[100]

[98] FTC Comm'r Christine S. Wilson, *A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Legislation,* Remarks at the Future of Privacy Forum (Feb. 6, 2020), at 14, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf.

[99] Comments of the CCIA, *Digital Advertising Business Guidance Publication*, File P114506 *(*Aug. 2, 2022), at 2.

[100] Stephanie A. Joyce, Remarks at the FTC Commercial Surveillance and Data Security Public Forum (Sept. 8, 2022.

Hartzog and Richards note that if laws limit certain types of business activities, the pace of innovation may slow, and costs may increase.[101] Any legislation or guidance should continue to be provided in broad strokes, setting forth principles rather than prescriptions. Overly prescriptive rules might inadvertently give advantage to firms by erecting barriers to entry as well.[102] In a hearing about the FTC's approach to consumer privacy, Commissioner Slaughter notes that developing a national privacy framework necessitates balancing competition and privacy goals.[103] She emphasized that we must take care that in attempting to secure increased protection for consumer data privacy, we don't inadvertently further entrench incumbents or otherwise hinder competition and choice.[104]

Thus, when legislation gets too prescriptive, it risks locking in existing technology and practices. As such, it is important that any privacy legislation introduced remain technology-neutral and flexible, which gives regulations the ability to continue to operate effectively as technology evolves. This flexibility enables two kinds of innovation: innovation in the online apps and services that consumers use and innovation in the means of protecting consumer data. In addition, flexibility and a focus on policy goals, not minute instructions, ensure a much longer shelf-life for any regulatory regime. As Commissioner Olhausen observed in a 2014 article, "Prescriptive ex ante regulation faces significant knowledge-gathering challenges because as a regulated industry continues to evolve, collected knowledge can quickly become stale. Obsolescence is a particular concern for fast-changing technological fields like telecommunications."[105]

Rules that become quickly obsolete require constant updating, sapping an agency's resources and destroying regulatory certainty. CCIA therefore encourages the Commission, if its forthcoming analysis finds that any additional rules for consumer privacy are warranted, to focus

---

[101] Wilson, *A Defining Moment,* at 13 (referencing Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1, 8).
[102] *See id.*
[103] *See* Tr. of FTC Hr'g, *The FTC's Approach to Consumer Privacy* (Apr. 10, 2019), at 132, https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf.
[104] *See id.*
[105] Maureen K. Ohlhausen, *The Procrustean Problem with Prescriptive Regulation*, 23 COMMLAW CONSPECTUS: J. OF COMMC'NS L. & TECH. POLICY 1 (2014), https://scholarship.law.edu/commlaw/vol23/iss1/2.

on consumers' rights and welfare, as well as the longevity and vibrance of the online ecosystem, rather than on specific methodologies and technologies that might achieve these outcomes.

III. Conclusion

As it evaluates whether to promulgate a rule related to online privacy and security practices," the Commission should consider whether the practices discussed in the ANPR satisfy its statutory obligations and constraints, whether the Commission's existing precedent and guidance sufficiently address those practices, and whether attempts to impose new rules for those practices would limit competition, innovation, and create additional regulatory uncertainty.

Respectfully submitted,

Stephanie A. Joyce
Chief of Staff and Senior Vice President
Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
stephaniejoyce@ccianet.org
amaranon@ccianet.org

November 21, 2022