Comments of the Software & Information Industry Association
Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security
Federal Trade Commission

November 21, 2022

Introduction

The Software Information Industry Association (SIIA) thanks the Federal Trade Commission (the "FTC" or "Commission") for the opportunity to provide this written comment on its Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security (ANPR).[1] SIIA is the principal trade association for those in the business of information, representing over 450 companies involved in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. SIIA's mission is to protect the three stages of the information lifecycle: creation, dissemination, and productive use.

The subjects covered by the ANPR are central to each phase of that lifecycle, and SIIA has followed the ANPR with interest since its inception. SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. Data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will not only ensure smooth implementation of uniform data privacy practices but provide a stable and robust environment for the information industry to flourish.

The Commission has historically been critical to preserving that environment. We recognize the important role the Commission has in fostering fair business practices in the digital economy and cracking down on deceptive and unfair practices.[2] Our member companies have long supported increased funding for the Commission to do this important work and view the Commission as a primary protector against fraudulent or deceptive conduct. And the Commission's work is at its strongest when it targets its limited resources at business practices that cause consumer harm.[3] The ANPR falls well short of this historical practice.

Part I of this submission addresses the Commission's authority to pursue the expansive rulemaking contemplated by the ANPR. The Commission's framing of the ANPR around

---

[1] FTC, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022) [hereinafter "ANPR"].

[2] See, e.g., ANPR at 51,276-80 (discussing the FTC's current role and rulemaking authority); id. at 51,286-92 (statements of Commissioners Khan and Slaughter).

[3] The ANPR notes that past enforcement actions have been brought for harm including practices that "pose risks to physical security, cause economic or reputational injury, or involve unwanted intrusions into consumers' daily lives." ANPR at 51,278.

"commercial surveillance" indicates a predisposition against a range of practices in the digital space that benefit consumers and are undertaken in accordance with the law. We are concerned that the Commission's use of "surveillance" – a term derived from law enforcement and national security contexts – to characterize these practices, if used as a foundation for eventual rulemaking, will draw significant legal challenges and ultimately undermine consumer protections and benefits. In addition, the Commission's statutory authority to regulate unfair or deceptive acts or practices in or affecting commerce[4] does not provide a blank slate to regulate the entire information economy. That authority is more circumscribed and expansive rulemaking would run against the Supreme Court's major questions doctrine.

In Part II of this submission, we provide specific recommendations concerning four subject matters covered by the ANPR – harms to children, data minimization and purpose limitations, automated systems, and digital advertising.

PART I: SCOPE AND POSTURE OF THE COMMISSION'S PROPOSED RULEMAKING

A. The Commission's Definition of "Commercial Surveillance" Encompasses the Entire Information Economy, which is Beyond Its Power to Regulate

The Commission has framed this rulemaking process as one involving "commercial surveillance." The ANPR defines "commercial surveillance," to include "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information,"[5] and includes "information that consumers actively provide" and "personal identifiers and other information that companies collect," and likens the private entities that participate in the digital environment to government actors collecting information for law enforcement or national security purposes.

Many questions in the ANPR focus on how, if at all, data-related practices harm consumers or increase the risk of harm to consumers; others request information about business models that could incentivize bad actors and lax practices.[6] Some of these harms (such as those that come from the classic "bait and switch") are well within the Commission's historic powers to ameliorate. But data now is part of every piece of interstate commerce and covers the entire economy. That reach is beyond ambitious: it is impractical, unwise and unworkable. Likely consequences include, among others, the following:

- sweeping in large swaths of publishers and providers of data that are protected by the First Amendment, which in turn would curtail free speech;

---

[4] See Federal Trade Commission Act, 15 U.S.C. §§41-58, as amended ("FTC Act"), at §45.

[5] ANPR at 51,277.

[6] E.g., id. at 51,281 (Questions 4 and 11 under *Harms to Consumers*).

- stifling beneficial activities that may be included, which could have repercussions on future innovative uses and restrict positive uses and benefits to consumers[7]; and

- devising unclear rules that could muddy the operations for the use of data for the business-to-consumer (B2C), business-to -business (B2B) and business-to-government (B2G) landscape, which will undermine market growth and development.

The overbreadth of the proposed definition will frustrate the Commission's regulatory goals, as it has neither the staff nor the authority to regulate consumer data use at such scale. When developing a rule on "commercial surveillance" and data security, the Commission should both recognize and account for the nuances across industries and data processing entities and target regulation at clearly unfair or deceptive acts and practices.[8] . That goal is not only ill-advised, it lies beyond the Commission's statutory authority.

B. The Commission's Authority Requires Narrowly Tailored Rulemaking

The breadth of the questions and the definition of "commercial surveillance" suggest that the Commission is considering rulemaking covering a wide range of practices that exceed the Commission's statutory authority. Indeed, the Commission appears to acknowledge this, noting among its "Reasons for Rulemaking" that Section 5 of the FTC Act does not provide authority to seek certain penalties, remediate certain alleged harm, and take action for harm that may be "opaque."[9] We recommend that the Commission focus on rules tailored to address prevalent unfair or deceptive acts or practices, lest its rule implicate the major questions doctrine.

In today's world, data – the subject of the ANPR – is central to our lives and underpins the American and global economies. Data impacts our daily lives in more ways than we can appreciate, including our entertainment, healthcare, shopping, travel, safety, news, and employment. At the same time, many companies "now have data at the core of their business models," as "data has become a key input in modern economic production alongside land, capital, labor, and oil."[10] Any national data regulation will directly impact every person and company in America.

The Commission's powers are not so broad. Congress limited its authority through the FTC Act. More specifically, sections 5 and 18 of the FTC Act authorize the Commission to regulate unfair or deceptive acts or practices and to engage in rulemaking in specifically drawn

---

[7] Cf. ANPR at 51,282 (Questions 24, 29).

[8] Moreover, the Commission's own guidance runs counter to the ANPR's framing of "commercial surveillance." The Children's Online Privacy Protection Act Frequently Asked Questions *encourages* companies to engage in what may be defined as "commercial surveillance" to prevent a child from back-buttoning to lie on a company's neutral age screen. See FTC, Complying with COPPA: Frequently Asked Questions.

[9] ANPR at 51,280-81 ("Reasons for Regulation").

[10] Yan Carrière-Swallow et al., The Economics of Data, imf.org (Sep. 23, 2019).

situations.[11] Section 5 authorizes the Commission to declare an act unlawful 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."[12] Section 18 authorizes the Commission to engage in rulemaking regarding unfair or deceptive acts or practices only where it "has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent."[13] In undertaking rulemaking, the Commission must analyze "the projected benefits and any adverse economic effects and any other effects, and of the effectiveness of the proposed rule and each alternative in meeting the stated objectives of the proposed rule."[14]

This language, which is historically focused on unfair or deceptive acts or practices and certain kinds of competition concerns, does not represent a Congressional invitation to regulate every use of data. The Supreme Court has invalidated rules that would have an expansive effect and significantly impact the nation's economy unless Congress has explicitly empowered the agency to do so.[15] This principle, referred to as the "major questions" doctrine, functions as a limit on agency action designed to protect principles or separation of powers in the absence of clear Congressional intent. Evidence of that intent is lacking.

For example, the Federal Trade Commission Improvements Act of 1980 added new requirements to the FTC Act to protect against improperly overbroad rulemakings. The 1980 Act included requirements that the Commission submit proposed rules to congressional oversight committees which "define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce"[16] and raises the level of judicial review to require that the rulemaking be supported by "substantial evidence" in the rulemaking record.[17] The text, structure, purpose and history of the statute limit the FTC's rulemaking power to cases in which consumers suffer substantial harm from particular, demonstrated unfair and deceptive practices. The existence and use of "commercial surveillance," in and of itself, is not intrinsically harmful or deceptive, and regulations that categorically treat it as such will likely be invalidated.

C. The Commission Should Focus on Areas Within Its Historic Areas of Expertise and Recognize that Congress is Acting

While the ANPR cannot and should not cover the scope of "commercial surveillance," we do believe that the Commission can successfully act to fill gaps in existing regulation. Such a

---

[11] FTC Act at §45, §57a.

[12] Id. at §45(n).

[13] Id. at §57a. (b)(3).

[14] Id. at §57(b)(C).

[15] See West Virginia v. Environmental Protection Agency, 2022 WL 2347278 (U.S. June 30, 2022) (W. Va. v. EPA).

[16] FTC Act at §57a(a)(1)(B).

[17] Id. at §57a(e)(3)(A).

focus would enable the Commission to leverage its limited and already overtaxed resources by focusing on practices that have been clearly demonstrated to create consumer harm.[18]

As the Commission recognizes, a robust regulatory framework governs data collection and use on a sector-by-sector basis.[19] Data use in the financial services industry, healthcare, education technology and other sectors are already regulated by a myriad of sector-specific laws and regulations (e.g., Gramm-Leach-Bliley Act; Health Insurance Portability and Accountability Act; Federal Educational Rights and Privacy Act; and more).[20] Acknowledging existing law facilitates certainty and compliance without the negative externalities that would accompany general economy-wide rulemaking.

Congressional activity also supports circumspection by the Commission. As Commissioner Phillips has noted, the Commission has suggested waiting on Congress with regard to the direction of children's protections, and it would be beneficial for the Commission to follow the same course with regard to the American Data Privacy and Protection Act (ADPPA) or other federal data privacy legislation.[21] The ADPPA, or H.R. 8152, represents a bipartisan and bicameral effort to regulate consumer privacy. Notably, the legislation establishes additional funding and resources for the FTC to support its effort and to expand its expertise. The FTC should continue to support Congress's efforts to advance legislation to create a national data privacy standard rather than potentially duplicating efforts and creating conflicting requirements through a privacy rulemaking.

One such area of duplication is biometrics,[22] where we respectfully urge the Commission to collaborate with other agencies on existing policy efforts before undertaking potentially redundant efforts outside its expertise. For example, earlier in the year, the White House Office of Science and Technology Policy (OSTP) sought information from the public on the uses and potential regulation of biometrics.[23] In parallel, the National Telecommunications and Information Administration (NTIA) held a listening session[24] on privacy and civil rights. SIIA has already shared input on these topics.[25] The Commission should not be single handedly addressing these issues in a vacuum. SIIA addresses particular sectoral concerns below.

---

[18] See Interview with Commissioner Rebecca Slaughter at the 2022 Politico AI & Tech Summit, (Sep. 29, 2022).

[19] See, e.g., ANPR at 51,281 (Question 12).

[20] See, e.g., FTC, Report to Congress on Privacy and Security (Sept. 13, 2021).

[21] ANPR at 51,296.

[22] Id. at 51,283 (Question 37).

[23] OSTP, Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56300 (Oct. 8, 2021).

[24] NTIA, Virtual Listening Sessions on Personal Data: Privacy, Equity, and Civil Rights (Jan. 3 2022).

[25] SIIA, Submission to OSTP on Biometrics (Jan. 14, 2022).

PART II: COMMENTS ON SUBJECT MATTER AREAS FOR POTENTIAL RULEMAKING

In each of the areas that follow, we recommend the Commission carefully consider the efforts and actions underway by other agencies and legislation introduced by Congress before undertaking rulemaking dedicated to these subject matters. Our overarching concern about the use of the term "commercial surveillance" applies throughout and we incorporate comments on this topic raised earlier in the submission.

A. Considerations of Potential Rulemaking Relating to Students and Children

i. Rulemaking on children and student privacy would be duplicative of existing Commission efforts.

We believe that new Commission rulemaking about the potential for harm to children and minors from the misuse of data is unnecessary.[26] The Commission has already embarked on a rulemaking process for the Children's Online Privacy Protection Rule (COPPA). That rulemaking effort, which began over 40 months ago,[27] is the appropriate vehicle to provide the public with specificity on what conduct constitutes unfair or deceptive acts or practices with respect to children and lies within the FTC's statutory authorization.

The new rulemaking duplicates efforts already underway as part of the Commission's COPPA policy work,[28] the U.S. Department of Education's efforts implementing Family Educational Rights and Privacy Act (FERPA), and other existing legal and regulatory frameworks protecting child and teen privacy in the education space. The Commission is working at cross purposes with itself by regulating subject matter as broad, vague, and untested as contemplated in the ANPR, instead of acting within those areas in which the Commission has both expertise and authority.

SIIA has long represented the educational technology industry before policymakers. Our members build cutting-edge tools used by learners, teachers, and school administration to access curriculum, communicate with each other, track attendance, and more. These companies typically work at the direction of schools–public and private, K-12 and post-secondary–and are under strict and overlapping obligations to protect the privacy and security of data. Businesses building products for use in America's schools have long been awaiting clarity from the Commission on the intersection of COPPA and FERPA. The rule review, which began in 2019, contemplated this intersection which was also recognized by the Commission in a 2017 workshop. The FTC took an important step in the recent policy statement on COPPA,[29] which SIIA applauded. The

---

[26] See ANPR at 51,281-82 (Questions 13-16, 22, 28).

[27] See FTC, FTC Seeks Comments on Children's Online Privacy Protection Act Rule (July 25, 2019).

[28] Children's Online Privacy Protection Rule ("COPPA"), 16 C.F.R. Part 312 as amended.

[29] Id.

Commission should continue to work on COPPA rule review and build on the fruitful efforts it has taken to ensure children's protections. The Commission has already collected nearly 180,000 comments to research the subject.[30] As discussed in more detail below, that area is already heavily regulated.

ii. Existing student data privacy laws and regulations already cover most areas of Commission concern.

There are a number of unique considerations for schools and education technology vendors that need to be carefully considered alongside the questions in the ANPR. First, existing federal and state laws afford a uniquely defined role for data processors and controllers in the education ecosystem. This coverage includes the Family Educational Rights and Privacy Act (FERPA) and the over forty states that have passed student privacy laws (such as the Student Online Personal Information Protection Act (SOPIPA)).[31] These laws establish rules for how schools may provide access to student data and how companies need to treat that information. As in other sectors, these separate roles are unique and limit the type of processing and use that the data processor has.

FERPA restricts how schools may share student education records and student personally identifiable information as a condition of receiving federal funds.[32] FERPA therefore governs most public K-12 schools, some private K-12 schools, and most public and private institutions of higher education. Substantively, FERPA generally requires affirmative parental consent before any release of a student's personal information and provides parents with the right to inspect educational records, and challenge inaccuracies in those records in appropriate circumstances.[33]

Narrow exceptions to the consent requirement exist that enable key educational functions. For example, FERPA's "school official exception" allows schools to outsource institutional services or functions to contractors (e.g., bus drivers), volunteers, or other third parties but only if those actors perform a function that would otherwise be done by school employees. In addition, the school must *directly* control such an actor's use and maintenance of education records, and the school is responsible to ensure that such an actor only uses personally identifiable information for narrow and school-related purposes for which the information was disclosed.[34] Finally, if the school is using the school official exception to disclose information without consent, it must tell parents about the fact that the school is using the exception.[35] Consequences for both an ed tech company and the school of any privacy violation are severe: If a vendor violates the non-

---

[30] FTC, Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule (July 25, 2019).

[31] See, e.g., Student Privacy Compass, studentprivacycompass.org (accessed Nov. 17, 2022); Ed Tech - Student Privacy Pledge, studentprivacycompass.org (accessed Nov 17, 2022).

[32] See the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99;

[33] See id. at 20 U.S.C. §1232g.

[34] Id. at 34 CFR Part 99.31(a)(1)(i).

[35] Id. at 34 CFR Part 99.31(a)(1)(ii).

disclosure requirements of FERPA, the school cannot provide access to personal information for at least five years.[36]

As FERPA is the floor for student privacy laws, states have passed laws to supplement FERPA's protections. A California law, for example, mandates that contracts between schools and ed tech companies bar ed tech companies from using student records for purposes other than those permitted by that contract and a prohibition on using student data to engage in targeted advertising. These laws also restrict selling of student data, amassing a profile of a student (except to provide the services), or disclosing student data except in limited authorized ways. Similarly, the laws have provisions mandating reasonable security procedures and practices to protect student data information from unauthorized access, use, destruction, modification, or disclosure. Over forty states have passed similar laws in the past decade.[37]

The Commission must consider the existing education laws and guidance in place, before developing any new rules about student data uses for educational purposes. Additionally, the Commission should work with the U.S. Department of Education and education stakeholders to understand the U.S. educational system and the impact any rulemaking might have on public and private K-12 and higher education institutions.

iii. Rulemaking must not curtail technology that benefits children.

SIIA's educational technology members operate in an extensively regulated data ecosystem: the American education system. That system not only provides America's learners with foundational education, educators with tools to do their job, and parents with access to information about what goes on at school but also often provides wraparound services like school lunches to meet the needs of students. This system has provided a number of tangible benefits of which data plays a key role.

Data is also essential to ed tech that helps students and teachers. One of the many examples include: End-to-end assessment platforms that allow teachers to focus on teaching the substantive requirements rather than focusing on checking for plagiarism, assessing manually, and then hand-grading. Each of those items, and many others, take time and effort and advancing education technology in those areas saves that time and effort and, in turn, helps teachers and professors focus more on teaching which, of course, benefits the students.

---

[36] Id. at 20 U.S.C. §1232g(b)(4)(B). The Department of Education has supplemented FERPA's statutory and regulatory provisions with guidance on using education technology in the classroom that clarifies best practices on how schools should effectively exercise direct control over the use and maintenance of education records and related PII by education technology companies. These practices include suggestions for data deletion and destruction, a process to facilitate parental access to the information through the school, and requirements to use personal information only for purposes outlined in the agreement with the school. See Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, studentprivacy.ed.gov (Feb. 2014); Protecting Student Privacy While Using Online Educational Services: Model Terms of Service, studentprivacy.ed.gov (Mar. 2016).

[37] See, e.g., Student Privacy Compass, studentprivacycompass.org (accessed Nov. 17, 2022); Ed Tech - Student Privacy Pledge, studentprivacycompass.org (accessed Nov 17, 2022).

The use of educational and student data gleaned from these education technology tools (which, as discussed above, is under the control of the contracting school district) is critical to a variety of policy decisions. For example, the U.S. education system makes federal funding decisions using education data and education records. Identifying inequities in education is often done through access to student data, including broader federal programs, such as the Free and Reduced Price Lunch program as well as vital state programs. Maintaining access to and use of that data affects a host of different policy interests beyond consumer protection.

Similar concerns exist with respect to the integrity of the education system itself. For example, the ANPR discusses whether children should have the ability to erase their own data.[38] FERPA enshrines the right of parents and eligible students to access and amend the education record and outlines a specific process in the regulations to do so.[39] This intends to ensure the integrity of the education record but does not grant parents and eligible students the right to delete things like grades, attendance records, and other data. The development of the educational record informs other critical data elements and policy efforts, including student attendance, important data elements that are integral and impactful for completion of curriculum requirements, federal school lunch program funding and more. School districts and their stakeholders – administrators, teachers, vendors, and parents – depend on the education data to make decisions on student outcomes and evaluate the impact of curriculum. Policy decisions involving a student or parent's access and amendment rights to an education record should reside with the U.S. Department of Education through its administration of FERPA, not the FTC.

B. Considerations on Potential Rulemaking Regarding Data Minimization and Purpose Limitations

The ANPR seeks input on data minimization practices, which it includes as part of the definition of "data security,"[40] and a range of potential purpose limitations on the collection and use of data. While we support inquiry into these important issues, we would urge caution with any potential rulemaking. Commission regulations on data minimization and purpose limitations would generate substantial risks to the information economy, innovation, and efforts underway to improve data fairness and equity and data-driven solutions to social needs and societal challenges.

i. Rulemaking on data minimization and purpose limitations would be overbroad and lead to negative consequences for businesses and consumers.

Creating national formal requirements for data minimization and purpose limitations is a task best suited to Congress. If the Commission chooses to focus on this area, we recommend that it develop best practice guidance focused narrowly on harms from improper data collection and retention. If it instead seeks to publish a rule that does not focus on data minimization principles that are carefully crafted and with consideration for the unique innovation economy in the United

[38] ANPR at 51,282 (Question 14).

[39] 34 CFR §99.20 et seq.

[40] ANPR at 51,277 ("The term 'data security' in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices.").

States, we fear it will have a chilling effect on the ecosystem, because it will hamper new product development, innovation, and could potentially limit free speech, and increase the risk that the regulation will be struck down in the courts.[41]

General purpose data use, in and of itself, has socially beneficial uses. These include market research, product development, financial analysis, support for national security and law enforcement, and more. Presuming harm in all data practices fails to distinguish between positive and unfair and deceptive data uses. Any proposed rulemaking should remain flexible in its approach toward data minimization and distinguish between controller and processor obligations toward the data.

In addition, rulemaking on these issues in absence of a congressional mandate will exacerbate the existing patchwork of data protection rules across the United States and generate significant uncertainty for consumers and compliance challenges for businesses.

We also caution the Commission on building a rulemaking that would unintentionally seek to conflate or combine "data minimization" and "purpose limitation" - which are separate but related concepts. "Data minimization" refers to implementing guardrails to restrict specific data processing and retention measures. In contrast, purpose limitations set concrete expectations on the specific uses of data for specific contexts. For example, under Virginia law, a business may be required to ensure the data it collects is reasonable and proportional to the disclosed purposes for which it is processed (unless the business obtains consent) and the business would be expected to discard the data it processes, subject to a specific retention schedule. This is data minimization. In California, a business may use (without obtaining consent) for a specific, exhaustive list of purposes, as detailed by the California Consumer Privacy Act, and the modified draft regulations that are now being finalized. The Commission's questions under *Collection, Use, Retention, and Transfer of Consumer Data* include a series[42] requesting feedback on data minimization and purpose limitation in the same breath, even though compliance with each may occur separately.

ii. Practical guidance, rather than rulemaking, would provide flexibility and a test bed to assess the value of specific rules around data minimization and purpose limitations.

We believe that guidance reflecting a risk-based approach to data minimization and purpose limitation will create productive guardrails for the collection and processing of data, elevating priority review of the highest risk activities. This type of guidance would be beneficial to stakeholders because it would further support the existing state level policies and industry standards. It would be similar in nature to the guidance on purpose limitation issued by the UK Information Commissioner's Office.

Furthermore, the United States has an opportunity to learn from the shortcomings of the GDPR. Research suggests that the GDPR's blanket opt-in consent regime has led to consumer

[41] This also relates to Questions 24 and 29 of the ANPR under *Costs and Benefits*. Id. at 51,282.

[42] See ANPR at 51,283 (Questions 43- 47).

consent fatigue, shrinking markets, and negative economic repercussions on product development and the innovation economy.[43] To the extent that the Commission elects to address data minimization and purpose limitations, it should ensure that such limitations are consistent with First Amendment guarantees and do not restrict socially beneficial use cases that are in the public interest.

For example, many of our members rely on publicly available information to generate productive and socially beneficial uses of products and services (e.g., finding missing children, performing corporate due diligence, preventing money laundering and fraud, and more). The policy benefits that result from a robust public domain are guaranteed by the First Amendment of the U.S. Constitution. We would recommend that any guidance the Commission may issue excludes publicly available information from its scope and correctly define that term to encompass information lawfully acquired from the government or contained in widely distributed media.

iii. Incorporate recommendations on privacy protective technology solutions to advance responsible data sharing and data rights within the data ecosystem.

While data minimization is one approach to limiting consumer harm, the Commission would benefit from considering the existing and emerging array of solutions and technologies that are permeating the ecosystem to ensure appropriate safeguards on the processing and sharing of consumer data. Examples of these solutions include the development of privacy by design programs, global privacy control, and recent opportunities for privacy-enhancing technologies, a range of policy solutions that embed data minimization into their approach. Privacy engineering programs are growing and many companies - from the largest household platforms to the newest startups - are using privacy preserving technologies to streamline the responsible sharing of personal information to unlock analytics that require strong privacy protective practices.

Companies are also using digital platforms to ensure compliance with data subject access requests, or "DSARs" - which are now fundamental to the individual rights guaranteed in state consumer privacy laws. Automated DSARs streamline the process businesses use to configure consumers' data subject rights and can expedite processing and response to these types of requests. The GDPR also defines such individual consumer data rights.[44]

Before pursuing rulemaking, we recommend the Commission consider the research and potential of these technologies in limiting the harms to consumers, as it is being further reviewed and shaped by the National Institute of Standards and Technology (NIST), OSTP, and an active interagency task force, to determine whether a rule in the data minimization arena would

[43] Rebecca Jansen et al., GDPR and the Lost Generation of Innovative Apps, National Bureau of Economic Research (May 2022).

[44] Chapter 3, Rights of the Data Subject, EU General Data Protection Regulation (GDPR), Regulation (EU), 2016/679 O.J. 2016 L 119/1.

potentially handcuff the testbed for these types of solutions, which are strong approaches to data minimization.[45]

C. Considerations on Potential Rulemaking Regarding Automated Systems

The ANPR also requests input[46] on automated systems. As an initial matter, we question whether there is a sufficient basis for the Commission to pursue rulemaking on automated systems. Although there are certainly context-specific instances in which an automated system could engage in an unfair or deceptive act, the suggestion that such systems are inherently unfair or deceptive is unsupportable. As former Commissioner Phillips noted recently, there is a "conspicuous lack of enforcement actions" for facial recognition or automated decision making and the Commission "never found that the use of facial recognition technology or automated decision-making themselves to be unfair."[47]

i. Review the evidence-based benefits of automated systems, which are embedded in routine practices across a diverse array of industries and use cases.

Today, virtually all computer-based activities involve algorithms, and both Congress and the Executive Branch are examining the effects of AI on all facets of economic and political life.[48] Congress has also begun to shape legislation on this subject in the Algorithmic Accountability Act of 2022,[49] and significant portions of the ADDPA also address it. And NIST is currently assessing input about emerging technologies and the impact of those technologies on the economy.[50] Without gainsaying the Commission's ability to engage in some targeted regulation within the scope of its mandate, it is Congress that must legislate across the entire economy.

---

[45] Comments of the Software & Information Industry Association (SIIA) on the Request for Information on Advancing Privacy - Enhancing Technologies, Submitted to the Office of Science and Technology Policy and the Fast Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics of the Subcommittee on Networking and Information Technology Research and Development, SIIA.net (Aug. 2022); Comments of the Software & Information Industry Association (SIIA) on the Request for Information: Study to Advance a More Productive Tech Economy, Submitted to the National Institute of Standards and Technology (NIST), SIIA.net (Feb. 14 2022).

[46] ANPR at 51,283-84 (Questions 53, 55-57, 67-69).

[47] ANPR at 51,295.

[48] E.g., Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, Office White House Office of Science and Technology Policy (OSTP), whitehouse.gov (Oct. 2022); The Biden Administration Launches the National Artificial Intelligence Research Resource Task Force, whitehouse.gov (June 10, 2021).

[49] H.R. 6580, 117th Congress (2021-2022). SIIA provided input on that legislation as well. Letter of the Software & Information Industry Association (SIIA) to the Subcommittee on Consumer Protection and Commerce Concerning H.R. 6580 - the Algorithmic Accountability Act of 2022, (Feb. 28, 2022).

[50] Study to Advance a More Productive Tech Economy, National Institute of Standards and Technology (NIST), 86 FR 66287 (Nov. 22, 2021).

ii. Leverage a risk-based approach for automated systems.

The GDPR provides some useful touchstones for the regulation of automated systems. . Article 22 requires analysis of systems that have a legal or similarly significant impact.[51] In those cases, data controllers must implement suitable measures to safeguard data subjects' rights, freedoms, and legitimate interests. Implementing a similar process in the United States would allow interoperability between U.S. privacy regimes and other countries without unintentionally stifling innovation and new product development. Its generation of consent fatigue notwithstanding, the GDPR does incorporate key aspects of risk-based policymaking that the Commission would be well-advised to incorporate into the regulation automated systems that cause the kind of harm the Commission is empowered to prevent.

We recommend that any regulation of automated systems should, to the maximum extent possible, be both risk-based and technology-neutral and be informed by several guiding principles.[52] These principles include:

- Distinguishing between automated systems and automated decision-making technology, to ensure the Commission is aware of nuances between regulating *decisions* that are generated by automated processes vs. regulating the technology itself.

- Evaluating decisions based on their impact on a natural person's rights - an approach informed by Article 22 of the GDPR, which protects consumers from decisions "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[53]

- Tailoring the scope of regulation to the risks involved with a specific context that balances the risk of harm to the consumer caused by the importance of the decision and the technology's involvement in that decision versus the benefits to the public to permitting that use. Such an approach might involve the right of consumers to opt-out of particular use cases involving life-altering or particularly challenging situations, such as access to essential goods or services (for insurance, healthcare, criminal enforcement, or other related purposes and activities).[54]

---

[51] Article 22, Automated Individual Decision-Making, Including Profiling, EU General Data Protection Regulation (GDPR), Regulation (EU), 2016/679 O.J. 2016 L 119/1 (hereinafter "GDPR").

[52] *See generally* Comments of the Software & Information Industry Association (SIIA) on the Request for Information: Study to Advance a More Productive Tech Economy, Submitted to the National Institute of Standards and Technology (NIST), (Feb. 14, 2022) (setting forth these principles in more detail); Comments of the Software & Information Industry Association (SIIA) to the California Privacy Protection Agency (Nov. 8, 2021) (same).

[53] GDPR at Article 22.

[54] Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 *et seq.* (2021).

- Protecting intellectual property and innovation. We caution the Commission against requirements such as mandating access to internal privacy assessments conducted by companies. Internal assessments support research and development processes, can be considered proprietary in nature, and may expose trade secrets about the company's automated processes, algorithms, and other confidential information.

iii. Ensure any rulemaking accounts for the substantial public records on automated systems amassed by Executive Branch agencies

It is critical that any Commission actions in this space build on the substantial records already developed within the Executive Branch on automated systems. These include records reflecting public input by NIST,[55] in connection with the AI risk-management framework, and OSTP, in connection with a recent RFI on biometrics and input provided on the AI bill of rights.[56] Ensuring cross-government interoperability will mitigate the unintended consequences of overregulating the digital market economy and stifling innovation.

D. Considerations on Socially Beneficial Uses of Digital Advertising

As Commissioner Phillips noted in his dissenting statement to the ANPR, the Commission "has never brought a case alleging that targeted advertising is unfair."[57] Thus, we recommend that the Commission be mindful of proposing a blanket rule that would have ripple effects on businesses that depend on advertising as their lifeblood in the digital economy. As noted earlier, the industry is already underway in proposing responsible solutions – such as privacy protective technologies and global privacy control – to provide consumers more opportunities to make appropriate choices about their data and the ads they receive. These emerging solutions allow for responsible and safe data sharing, while keeping the advertising ecosystem intact. We encourage the Commission to balance the countervailing benefits to consumers before proposing sweeping changes to the digital ads ecosystem.,

First, the internet of today and the free online services made available to consumers are reliant on advertising, including personalized or targeted advertising. Targeted advertising is a widespread practice and not one that is the exclusive domain of large technology companies. Many U.S.-based retailers, for example, have their own ad networks and ad tech. Disrupting that advertising will unsettle business expectations based around widespread and accepted activity.

Second, overbroad rules will also harm small and medium-sized publishers and negatively affect consumer welfare. To the extent "commercial surveillance" includes personalized or targeted, an outright ban would effectively restrict or significantly disrupt the free ad-supported services consumers enjoy today. And contextual advertising, where advertisers are looking for the right context to target ads, has its limits, as it creates inherent benefits for larger publishers

---

[55] NIST, AI Risk Management Framework: Second Draft (Aug. 18, 2022).

[56] See OSTP, Notice of Request for Information (RFI) on Public and Private Uses of Biometric Technologies, 86 FR 56,300 et seq. (Oct. 08, 2021); OSTP Blueprint for an AI Bill of Rights (Oct. 2022).

[57] ANPR at 51,295.

with the most varied web presence, and inevitably leads to less revenue for smaller publishers and creators (such as bloggers, newsletter publishers, and video content creators) and developers. As publishers find it increasingly difficult to find contextually relevant advertisers, the diversity of online content will shrink and free information services will wither. Only the largest companies will be able to survive.

Third, consumers appear aware of the existence of targeted advertising, and data shows they welcome it. For example, there is data indicating that users prefer personalized advertising because it shows them ads relevant to their interests. A study by Infogroup found that 90% of consumers say that messages from companies that are not personally relevant to them are "annoying."[58]

Conclusion

For the foregoing reasons, we recommend that the Commission focus current efforts on developing guidance and best practices to inform data protection and security in the commercial context.

While there may be a need at some point for formal rulemaking, the breadth of the issues suggested by the ANPR and questions about the Commission's authority to undertake such expansive rulemaking counsel for a more measured and measurable approach.[59] For example, in 2020, the Commission published a report[60] that shared the outlook on data privacy and security, carefully considering the various policy positions and efforts that were underway. This type of effort would enable industry and civil society to more easily address guidance, allow for adjustments as technology develops, and ensure regulatory action remains consistent with statutory authorization.

In addition, we note the critical role of the Commission in consumer education. We note that the White House has undertaken an initiative to buttress efforts to elevate data security and cybersecurity by encouraging the adoption of digital labels for internet-of-things devices.[61] These "cyber labels" will allow consumers to judge a device's security for themselves. With its emphasis on protecting consumers by educating them, this is a perfect example of a task the Commission is well positioned to lead (and which could make a more tangible, positive impact with its already overutilized resources) than an expansive rulemaking effort.

---

[58] See Rimma Kats, "How's that Personalization Going?," Insider Intelligence (Jun. 13, 2019).

[59] Cf. SIIA Comments at the FTC's Commercial Surveillance and Data Security Public Forum, September 8, 2022(Sep. 9, 2022).

[60] Lesley Fair, Updating You on FTC Privacy and Data Security Initiatives, FTC.Gov (May 25, 2021).

[61] White House, Statement by NSC Spokesperson Adrienne Watson on the Biden-Harris Administration's Effort to Secure Household Internet-Enabled Devices (Oct. 20, 2022).

We would also urge the Commission to continue its current emphasis on enforcement actions. Such actions, as exemplified recently in the *Drizly* and *Chegg* matters, help to deter unlawful business conduct, sanction bad actors, and educate the public.[62]

Thank you for considering SIIA's comments. We look forward to working with the Commission as it considers potential rulemaking on issues raised in the ANPR.

[62] FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers, FTC.Gov (Oct. 24, 2022).