Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

COMMENTS

of

PRIVACY FOR AMERICA

on the

Advance Notice of Proposed Rulemaking for a
Trade Regulation Rule on Commercial Surveillance and Data Security
"Commercial Surveillance ANPR, R111004"

Counsel:
Stuart P. Ingis
Emilio W. Cividanes
Tara Sugiyama Potashnik
Rob Hartwell
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

November 21, 2022

I. Introduction and Executive Summary

Privacy for America is a coalition of top trade organizations and companies representing a broad cross-section of the American economy. We appreciate the opportunity to provide comments on the Federal Trade Commission's ("FTC" or "Commission") Advanced Notice of Proposed Rulemaking for a trade regulation on "commercial surveillance" and data security ("Privacy ANPR").[1]

Privacy for America, as demonstrated in our *Principles for Privacy Legislation* ("Framework"), supports the congressional creation of a national, preemptive, and comprehensive standard for consumer privacy that provides the Commission with resources to oversee privacy and data security issues.[2] Congress is best positioned, as the only governmental institution with the scope and authority through the democratic process, to debate and establish a national legal framework for the use of data in commerce that is responsive and workable for the entire U.S. economy. By contrast, the FTC's jurisdiction limits the Commission to issuing regulations covering only those entities subject to its statutory grant, and then only to acts or practices shown by substantial evidence to be prevalent and unfair or deceptive.[3] Additionally, any regulations the FTC issues in the privacy and data security area as an outgrowth of the Privacy ANPR would likely add to an increasing patchwork of existing regulatory requirements for companies and consumers to navigate.

The FTC should not cast itself as a quasi-legislature capable of regulating any activity it sees fit without a grounding in its congressionally granted authority. The more prudent path would be for the Commission to refrain from seeking broadly to regulate the entire U.S. data-supported economy while Congress is actively considering a comprehensive, preemptive standard. Instead of continuing with the rulemaking process, the Commission could support Congress's work by using the responses to the Privacy ANPR as a record for Congress to employ. This approach would help to remove the substantial procedural hurdles to exercising the expansive regulatory authority the Commission incorrectly asserts in the Privacy ANPR. At the very least, the Commission ought to narrow the focus of its Privacy ANPR to areas within its expertise, jurisdiction, and statutory grant of power as well as to practices shown by the FTC's own enforcement history to be prevalent and unfair or deceptive.

If the Commission nonetheless continues pursuing the rulemaking process it launched with the issuance of this broad Privacy ANPR, we provide comments addressing the following matters to contribute to the administrative record in this rulemaking proceeding: (1) the statutory deficiencies that exist in the Privacy ANPR and how those impact the rulemaking process; (2) the statutory and constitutional limits that restrict the Commission's rulemaking authority; (3) how the FTC should analyze potential harms and injury related to data privacy as well as how many practices outlined in the Privacy ANPR do not pass muster under the analysis we outline; (4) the myriad benefits the data-driven economy delivers to consumers and businesses, which the

---

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022) (hereinafter *Privacy ANPR*).

[2] Privacy for America, *Principles For Privacy Legislation*, https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/ (last visited Oct. 7, 2022) (hereinafter *Privacy For America*).

[3] *See* 15 U.S.C. § 57a; *see also* Section IV.

Commission omitted from the Privacy ANPR; and (5) the importance of a reasonable and flexible risk-based data security framework.

a. The Privacy ANPR is statutorily deficient and will not lead to the establishment of a sound administrative record.

Decades have passed since the Commission last undertook a Magnuson-Moss ("Mag-Moss") rulemaking on the scale presented by the Privacy ANPR. The Commission unfortunately does not follow the detailed requirements Congress imposed as a fundamental part of the Mag-Moss rulemaking process. Mag-Moss's requirements for the publication of an ANPR were established specifically to prevent the type of overbroad rulemaking reflected in this Privacy ANPR, which is centered on non-specific practices without "any reasonable belief that the alleged wrongdoing was prevalent in the marketplace."[4] The Commission fails the first step of the Mag-Moss process because this Privacy ANPR does not follow the statute by providing "a brief description of the area of inquiry under consideration, the objectives [it] seeks to achieve, and possible regulatory alternatives under consideration by the Commission."[5]

Even if the Privacy ANPR had met the initial Mag-Moss requirements, the ANPR cannot provide a path to the specific, clear, and fulsome administrative record needed for the FTC to declare an act or practice prevalent and unfair or deceptive supported by substantial evidence.[6] To perform the cost-benefit analysis necessary to declare a specific data practice unfair or deceptive and prevalent such that the FTC is able to issue a trade regulation, the Commission should request input from stakeholders on specific practices it believes meet those requirements. Instead, the Commission asks how it should define injuries, what practices it should regulate, and how those regulations should take shape. Rather than providing a framework for potential regulation and placing stakeholders on notice about potential future action, the Commission's Privacy ANPR is so vague and broad that it effectively allows the FTC to design any public policy outcome it wishes to accomplish. "Public policy" is exactly the type of "evidence" that Congress stated may not serve as the primary basis for declaring a practice as "unfair."[7] To create a useful administrative record that addresses identifiable practices, the Commission must drastically revise the Privacy ANPR.

b. The Commission is tightly restricted by statute and the U.S. Constitution regarding how it may regulate data practices in the marketplace.

The Privacy ANPR seeks comment on a variety of issues typically falling outside the FTC's purview or addressed through specific legislation passed by Congress. These areas

---

[4] 126 Cong. Rec. 11918 (statement of Sen. John C. Danforth). Apparently, the FTC takes issue with companies using data to "make money" and "sell more products," which is the basis of all commerce in the economy at some level. FED. TRADE COMM., FACT SHEET ON THE FTC'S COMMERCIAL SURVEILLANCE AND DATA SECURITY RULEMAKING at 1-2, https://www.ftc.gov/system/files/ftc_gov/pdf/Commercial%20Surveillance%20and%20Data%20Security%20Rulemaking%20Fact%20Sheet_1.pdf ("Companies may use some of the information they collect to provide products and services, but they can also use it to make money.").

[5] 15 U.S.C. § 57a(b)(2)(A)(i).

[6] *Id.* § 57a.

[7] *Id.* § 45(n).

include children's privacy through the Children's Online Privacy Protection Act ("COPPA"), where Congress provided clear authority to the Commission; and other areas where Congress has not provided a clear grant of authority for the Commission to regulate. The Commission's actions must be confined to those specific and limited areas where it has been provided authority by the Congress, and must always stay within the bounds set by the First Amendment and Constitution.

c. The Commission must focus on cognizable harms when determining whether conduct is unfair or deceptive.

The Privacy ANPR requests comment on types of conduct and injuries the Commission should seek to regulate and address. The Commission is statutorily bound to address only prevalent unfair or deceptive acts or practices, and part of this determination centers on the practice in question representing a real risk of substantial, unavoidable injury to consumers. The Commission should look to concrete standards, such as those used by the courts, to assess the types of injuries that can be addressed through rulemaking. A lack of cognizable, substantial injury is especially apparent with respect to routine and essential data practices, market research, data-driven advertising and personalization, third-party data services, practices with appropriate notice and choice, and employee and business-to-business data practices.

d. Data practices provide significant benefits to consumers and competition.

Data is a backbone of the modern, dynamic, and vibrant U.S. economy. Valuable and detailed economic studies demonstrate that the use of data in commerce improves the lives of consumers and creates a competitive marketplace. While the Privacy ANPR presumes that such data practices create harms and serve a limited value, the Commission must fully consider how any regulatory action would diminish or impede myriad benefits accrued to consumers and businesses alike through the collection, use, and sharing of data in commerce. These benefits accrue from practices, such as data enhancement, targeted advertising, fraud prevention, and various other practices, that help deliver free content and services to consumers and allow small businesses to compete in a dynamic marketplace supported by the responsible use of data. Not eliciting information about the benefits of data use—or even suggesting that the Commission has no interest in that type of analysis—can only undercut the administrative record needed for a final rule.

e. Flexible and risk-based data security frameworks are key to workable requirements.

When considering data security requirements, the Commission should take a risk-based approach. The Commission should avoid one-size-fits-all approaches. Such approaches would functionally prohibit small and new entrants into the data-driven marketplace from effectively competing due to compliance costs. Additionally, the Commission should not issue regulations regarding data breach notification to avoid overlapping and contradictory requirements with the 50-plus breach notification requirements already in place in every state, territory, and the District of Columbia.

II. The Privacy ANPR does not carry out Congress's mandate for FTC rulemaking.

The Commission's current attempt at a privacy rulemaking exhibits a disregard for how and why the Commission's limited rulemaking authority developed. Congress created the Mag-Moss rulemaking process in response to the Commission's activity in the 1970s that many viewed as controversial. At the time, the FTC flatly proposed banning children's advertising, which led many to accuse the Commission of acting as the "great national nanny."[8] Specifically, the 1980 appropriations for the FTC created the ANPR requirement for the Mag-Moss process. This statutory addition sought to stop the Commission from continuing to institute "[r]ulemaking ... without advance notice to affected parties and without any reasonable belief that the alleged wrongdoing was prevalent in the marketplace."[9] Congress also sought to prevent Commission activity "in areas where the Congress specifically reserved jurisdiction elsewhere."[10] The FTC has come closer to Congress's expectation of providing an actionable ANPR in recent memory, such as its rulemaking process regarding government impersonation.[11] However, with the Privacy ANPR, the Commission has chosen to engage in just the kind of open-ended, unstructured, and unsupported rulemaking process that Congress forty years ago sought to limit.

Any ANPR issued by the FTC must provide "a brief description of the area of inquiry under consideration, the objectives [it] seeks to achieve, and possible regulatory alternatives under consideration by the Commission."[12] Here, the Commission states in the Privacy ANPR that "commercial surveillance" refers to "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."[13] The Privacy ANPR fails to meet the statutory standard and is instead a virtually unlimited request for comment on almost any and all data practices that fuel the U.S. economy.[14]

While the balance of our comments attempts to respond to and provide cogent feedback on the inadequate Privacy ANPR, we believe it is important first to highlight flaws of the ANPR as it serves as the foundation for any related rulemaking. We discuss: (1) the Privacy ANPR's failure to define the scope of inquiry or to offer regulatory alternatives; (2) the Privacy ANPR's inability to produce a robust administrative record to satisfy Mag-Moss rulemaking requirements for specificity or a showing of unfairness or deception; (3) a record based on the Privacy ANPR would not support a finding of prevalence; and (4) the administrative record produced would not uphold a final rule that must be supported by substantial evidence in a court challenge. The FTC should ensure that the Privacy ANPR meets all steps Congress required the Commission to

---

[8] *See* 126 Cong. Rec. 11824 (statement of Rep. Jack Hightower (D-TX) that "No single activity or program undertaken by the Commission has been more difficult or more fraught with constitutional and due process hurdles than the so-called children's television rulemaking proposal"); J. Howard Beales III & Timothy J. Muris, *Return of the National Nanny*, WALL STREET J. (May 26, 2022), https://www.wsj.com/articles/return-of-the-national-nanny-ftc-activists-rulemaking-regulation-banning-mandates-illegal-11653596958; *see also* 125 Cong. Rec. 29745-55, 32454-84, 33665-82 (1979); 126 Cong. Rec. 2009-84, 2339-404, 9645-56, 11817-34, 11912-42 (1980).
[9] 126 Cong. Rec. 11918 (statement of Sen. John C. Danforth).
[10] *Id*.
[11] *Trade Regulation Rule on Impersonation of Government and Businesses*, 86 Fed. Reg. 72901-05 (proposed Dec. 23, 2021).
[12] 15 U.S.C. § 57a(b)(2)(A)(i).
[13] *Privacy ANPR* at 51277.
[14] This sentiment is echoed in Commissioner Noah Phillips dissent to the Privacy ANPR. *Privacy ANPR* at 51294.

undertake when it created the Mag-Moss process and focus on a narrower set of clear objectives if it chooses to continue its rulemaking effort.

a. The Privacy ANPR fails clearly to state the scope of potential inquiry or present possible regulatory alternatives, which will limit the utility of any administrative record for the creation of a final rule.

The extraordinary breadth of content and questions in the Privacy ANPR suggests that the Commission may proceed in any range of directions on the immensely significant issue of data's fundamental role in the modern U.S. economy.[15] However, the Federal Trade Commission Act ("FTC Act") limits the Commission's rulemaking jurisdiction under Mag-Moss to defining "with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce."[16] The Privacy ANPR fails to indicate which of the myriad data practices to which it alludes may be deceptive or unfair or how the Commission may subsequently address those practices.

For example, the Commission discusses varied areas of potential interest for regulation, but each of these topics alone represents an important and vast sector of the economy supported by data collection, use, transfer, and other processing activities.[17] The Privacy ANPR fails to identify what activities, practices, sectors of the economy, or other important aspects of the data-driven marketplace it is targeting as unfair or deceptive and ripe for regulation.

Without a clear description of which areas of the data-driven economy are subject to inquiry, commentors are unable to provide valuable feedback focused on the cost, benefits, and potential regulatory alternatives to the Commission's chosen path. Indeed, the Commission did not provide the required "possible regulatory alternatives" in the Privacy ANPR beyond vague questions about its power to limit or ban certain activities or to craft new forms of regulatory remedy like "algorithmic disgorgement."[18] As a result, the Privacy ANPR fails to create an effective pathway to building an adequate administrative record. The FTC should solicit clear and actionable information from stakeholders to produce a notice of proposed rulemaking ("NPRM") efficiently, effectively, and legally if it intends to develop a final rule that can withstand the statutorily mandated judicial review period.[19] The Commission should reconsider the Privacy ANPR as it is currently composed and determine if and how the FTC could provide a more coherent request for input through one of the various means at the Commission's disposal.

---

[15] Philips, *Privacy ANPR* at 51294; *see, e.g.*, *Privacy ANPR* at 51281 (Questions 1-12).
[16] 15 U.S.C. § 57a(a)(1)(B).
[17] *See generally Privacy ANPR* at 51274, 51276, 51277, 51280, 51281, 51283 (citing to data-driven content personalization; data-driven advertising; employee-employer relations; franchisee-franchisor relations; housing; credit underwriting; student data in the education context; third-party data service providers; social media use by teens and young adults; security breach notification; and data security standards as areas of interest).
[18] 15 U.S.C. § 57a(b)(2)(A)(i); s*ee e.g., Privacy ANPR* at 51285 (questions 83-94). This specific example of a potential regulatory approach is a prime example of the vague proposals in the Privacy ANPR that could result in stifling innovation and future consumer benefits flowing from responsible data practices.
[19] 15 U.S.C. § 57a(e).

b. The Privacy ANPR will not create the robust administrative record needed successfully to complete the Mag-Moss rulemaking process with the specificity required.

The overbreadth and general deficiencies in the Privacy ANPR not only fail to meet the statutory requirements for an ANPR, but they also consign the Commission to failure through the rest of the Mag-Moss process. To complete the Mag-Moss process and issue a compliant final rule, the FTC must find that specific acts or practices are unfair or deceptive and that they are prevalent in the marketplace such that a rule is necessary.[20] This finding must be based on the Commission's history of cease and desist orders or any other information available to it that indicates a "widespread pattern of unfair or deceptive acts or practice."[21] Due to its lack of precision and specificity, the Privacy ANPR does not facilitate effective stakeholder input on specific practices, potential regulatory frameworks, or other costs or benefits of potential Commission action. The administrative record produced will not allow the Commission to satisfy these required rulemaking steps. Such an administrative record and incomplete rulemaking process will undermine any potential final rule due to a lack of support from substantial evidence undergirding the FTC's determinations.

"Unfair or deceptive acts or practices" has a specific meaning under the FTC Act, and the Commission must rely on the administrative record created by its own actions and the Privacy ANPR to demonstrate that the standard is met when it declares a specific practice to be covered by a final rule. To establish that a practice is "unfair," the FTC must determine that the practice: (1) causes or is likely to cause substantial injury to consumers; (2) cannot be reasonably avoided by consumers; and (3) is not outweighed by countervailing benefits to consumers or to competition.[22] To establish that a practice is "deceptive," the FTC must determine that the practice: (1) misleads or is likely to mislead a consumer; (2) whose interpretation of the practice is reasonable; and that (3) the misleading practice, representation, or omission is material.[23] If the Commission is to declare that an aspect of the vast array of practices the FTC includes in its definition of "commercial surveillance" or "lax data security" is unfair or deceptive, the FTC must meet these standards. Yet the Privacy ANPR defines these terms so amorphously that the Commission neither identifies practices nor describes how the areas of inquiry may constitute unfairness or deception. Without more clarity, the Privacy ANPR is an ineffective vehicle for creating a meaningful administrative record of unfair or deceptive acts or practices.

Indeed, the FTC's rulemaking history shows that it must do more than create requirements to "prevent" unspecified unfair or deceptive practices in a particular industry or area of the economy. The ANPR process was established by Congress to help the marketplace ascertain what practices the Commission should identify as the appropriate area of inquiry. The Commission must ultimately define with specificity what conduct it considers to violate its statutory mandate.[24] Because the Privacy ANPR is so expansive and unfocused, stakeholders are

[20] 15 U.S.C. § 57a(b)(3); Rules and Rulemaking Under Section 18(a)(1)(B) of the FTC Act, 16 C.F.R. § 1.8 (2021).
[21] 15 U.S.C. § 57a(b)(3).
[22] *Id*. § 45(n).
[23] FED. TRADE COMM., POLICY STATEMENT ON DECEPTION (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[24] *See* Katharine Gibbs Sch. v. FTC, 612 F.2d 658 (2d. Cir. 1979).

unable to provide information and evidence to assist the Commission's inquiry into acts or practices that may be deceptive or unfair. Evidence that certain practices carry significant benefits that outweigh potential "harms" would better serve the Commission's rulemaking process. A revised Privacy ANPR that more clearly delineates what areas of inquiry the Commission believes should be the focus regarding alleged unfair or deceptive acts or practices could help elicit the responses needed to establish a robust administrative record. Absent that, the Commission will be very challenged in its attempts to promulgate a rule with the specificity required by the FTC Act.

c. The Privacy ANPR will fail to aid the FTC in establishing that any specific practices are "prevalent" in the marketplace.

As discussed below in section IV, the Commission's enforcement history does not support a finding of prevalence for many of the categories of supposedly harmful practices identified in the Privacy ANPR. This lack of enforcement history means that the FTC must rely on "other information available to the Commission [that] indicates a widespread pattern" of unfair or deceptive practices in order to meet the statutory requirement of prevalence.[25] The Commission must make this finding of prevalence when issuing an NPRM. Therefore, the administrative record created in the present proceeding will be key to justifying any future NPRM. It is in the Commission's best interest to issue a revised Privacy ANPR to better enable the FTC to make an adequate finding of prevalence.

d. The Commission is not a legislative body, and to survive judicial review a final rule must be supported by substantial evidence and fall within the FTC's statutory grant of authority.

Congress, as the national legislative body, is imbued with the broad authority to regulate the national economy through the Commerce Clause.[26] The Commission, however, was granted more limited authority by Congress to issue rules under Mag-Moss that regulate only unfair or deceptive acts or practices that are prevalent. In addition, the FTC's rulemaking procedure must meet all procedural and substantive requirements, and upon judicial review, must demonstrate that the rulemaking meets those requirements with "substantial evidence in the administrative record."[27] Unless the administrative record demonstrates substantial evidence to support a finding that specific data practices are unfair or deceptive in a widespread and prevalent manner, a final rule will fail any judicial review.

That very administrative record begins with the Privacy ANPR, and that record will be one of very few sources of authority for a final rule given that the Commission has no history of finding many of the data practices potentially subject to regulation mentioned in the Privacy ANPR to be unfair or deceptive, let alone prevalent.[28] The Commission should seek to establish

[25] 15 U.S.C. § 57a(b)(3).
[26] *See* U.S. CONST. art. I § 8, cl. 3 (Commerce Clause). Congress (like the FTC itself) is, of course, limited by the Constitution's other provisions, such as the First Amendment, in how it may regulate commerce. *See* U.S. CONST. amend. I.
[27] 15 U.S.C. § 57(e)(3); 126 Cong. Rec. 11918 (statement of Sen. John C. Danforth). Section III below further establishes the statutory and constitutional limits on potential rulemaking authority.
[28] *See Privacy ANPR* at 51295.

a robust, fulsome, and specific rulemaking record at the start of its process based on a revised Privacy ANPR if it seeks to complete the Mag-Moss processes within the bounds of its statutory grant of authority. Taking the time to reassess and focus on the specific practices the Commission believes are prevalent in the market and unfair or deceptive—such that an advance notice of proposed rulemaking could create a strong record—would be the most prudent course of action if the Commission insists on continuing down the Mag-Moss path instead of allowing Congress to continue its more appropriate legislative process developing national privacy legislation.

III. The FTC is bound by the U.S. Constitution and other laws that limit its jurisdiction and regulatory reach.

Throughout the Privacy ANPR, the FTC seeks comment on what may limit the Commission's regulatory authority within existing laws and the Constitution.[29] The FTC must respect the constitutional and statutory bounds of its authority in any proposed rulemaking. Overbroad rulemaking will trigger legal challenges that would likely overturn FTC action and waste its limited resources. In these comments, we discuss four such limitations on privacy rulemaking: (1) the FTC Act itself (discussed throughout); (2) COPPA; (3) the First Amendment; and (4) the major questions doctrine regarding appropriate agency actions.

a. COPPA bounds the FTC's authority to regulate kids' online privacy.

The Privacy ANPR asks a number of questions relating to data from children and teens.[30] On the subject of online privacy for minors, Congress authorized the FTC to regulate children's online privacy only for children younger than 13, and the FTC has no authority under Mag-Moss to reverse that congressional judgment. In a bill introduced just before COPPA was enacted as part of omnibus legislation, the sponsors included provisions relating to data collection from minors aged 13-16.[31] These provisions were not included in the version of the bill that was enacted.[32] Congress had the opportunity to include teen privacy in its regulatory mandate to the FTC, but it declined. Congress has had many opportunities since COPPA was enacted to expand the law to include teens but has consistently declined to do so.[33] Just prior to the announcement of the Privacy ANPR, the Senate Commerce Committee approved a bill that would, in part, raise the age of children covered by COPPA.[34] The FTC must respect Congress's authority in this area and not raise the age of children covered by COPPA or its implementing regulations.

The FTC has previously recognized that it is inappropriate to regulate data collected from teens and online services with broad appeal in the same way that it regulates children's data and has consequently rejected regulations that would expand the age group covered under COPPA's definition of "child."[35] Specifically, the FTC has recognized both the practical challenges in

[29] *See Privacy ANPR* at 51281-82 (questions 13-23); 51284 (question 40).
[30] *Id.*
[31] S. 2326,105th Cong. (1998).
[32] H.R. 4328, 105th Cong. (1998).
[33] *See, e.g.*, S. 748 116th Cong. (2019).
[34] S. 1628, 117th Cong. (2021)
[35] 76 Fed. Reg. 59804, 59805 (Sept. 27, 2011), https://www.govinfo.gov/content/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

expanding COPPA to cover teens and the potential for such an expansion to result in an unconstitutional limit on teen speech:

> The COPPA model would be difficult to implement for teenagers, as many would be less likely than young children to provide their parents' contact information, and more likely to falsify this information or lie about their ages in order to participate in online activities. In addition, courts have recognized that as children age, they have an increased constitutional right to access information and express themselves publicly. Finally, given that adolescents are more likely than young children to spend a greater proportion of their time on Web sites and online services that also appeal to adults, the practical difficulties in expanding COPPA's reach to adolescents might unintentionally burden the right of adults to engage in online speech.[36]

As a result, the Commission has stated that it "does not recommend that Congress expand COPPA to cover teenagers."[37] The Privacy ANPR fails to address any of these pitfalls of overregulating minors online, and it does not appear to respect the ability of those 13 and over to engage online through their own choices.[38]

The FTC should continue to consider unintended effects of regulations meant to protect children on adult or teen Internet users. A blanket expansion of COPPA's age limit, for example, would also harm adult Internet users. Because the interests of teenagers are often not meaningfully different from one age to another, most online properties would find it impossible to implement an effective filtering method without also preventing individuals sixteen and older from accessing that same valuable content online (such as important health, sexual orientation, and other information). Teens 13 to 17 may have good reason to want to access this same content without parental consent.

Privacy rulemaking should continue to allow teens to benefit from access to general information across the Internet as they mature and become capable of making critical decisions about access to constitutionally protected speech in an informed manner. Protections for minors 13 to 15 should balance the need to protect those individuals with the understanding that they—unlike children under 13 years of age—are capable of legally-recognized critical thinking and rational decision-making. Individuals in this age range need access to information to inform their decision-making and help build their point-of-view. Imposing broad regulations on general audience content could have the unintended effect of blocking access or deterring users from accessing valuable resources. As explained by the Seventh Circuit, those individuals under the age of 18 have a First Amendment right to access information they find of interest:

> [S]ince an eighteen-year-old's right to vote is a right personal to him rather than a right that is to be exercised on his behalf by his parents, the right of parents to enlist the aid of the state to shield their children from ideas of which the parents disapprove cannot be plenary either. People are unlikely to become well-

[36] *Id.* (internal citations omitted).
[37] *Id.*
[38] *Privacy ANPR* at 51281-82 (questions 13-23).

functioning, independent-minded adults and responsible citizens if they are raised in an intellectual bubble.[39]

In addition, we are concerned that the FTC is asking about parental control mechanisms other than parental consent. COPPA's parental consent framework was mandated by Congress. Any departure from this standard would run counter to the statute authorizing the COPPA Rule and would be a gross overreach. Such an action would be inappropriate without an express grant of authority from Congress.

Indeed, while the Commission cites to various concerns related to the mental health and social impacts that data personalization and targeted advertising practices may have on minors between 13 and 16, none of those potential harms appear to be remedied by the regulatory authority of the Commission.[40] Any potential injuries of this type that the Commission may read about in the media or hypothesize about are not the types of injuries that are cognizable under the FTC Act or that could sustain a challenge in court.[41] Additionally, the First Amendment's protections also extend to individuals in this 13 to 16 age range (including their First Amendment right to receive relevant advertising and content).[42] While the Commission may desire a certain policy outcome to be achieved with regard to those between 13 and 16 years of age, it is clear that Congress chose to limit the agency's authority to those under 13 and that the societal concerns cited in the Privacy ANPR are more appropriately resolved by Congress or civil society, not through Mag-Moss rulemaking by the Commission.

b. The First Amendment protects commercial speech implicated in the Privacy ANPR.

As the FTC considers further regulations on data use, including in advertising, the Commission should be mindful of the well-established constitutional protections for advertising and other commercial speech provided by the First Amendment. The Commission asks whether the First Amendment would bar the FTC from regulating the way that companies personalize advertising.[43] The short answer to this question is yes; the First Amendment bars any broad, generalized restrictions on advertising, targeted or otherwise. Courts have recognized advertising as protected commercial speech. In 1976, the U.S. Supreme Court struck down a law prohibiting pharmacies from advertising the price of medications, asserting that the First Amendment includes both the right of the speaker to speak *and* the right of the listener to receive information.[44] Overly broad restrictions on advertising would harm not only businesses but also consumers who would suffer from a lack of information about their potential choices in the marketplace. Small businesses rely on advertising to connect with existing and potential customers. In 2011, the Supreme Court struck down a restriction on the use of data by pharmaceutical research companies, manufacturers, and other third-party data suppliers because those restrictions were overly broad and did not directly advance a legitimate state interest

[39] American Amusement Mach. Ass'n v. Kendrick, 244 F.3d 572, 577 (7th Cir. 2001) (holding that a ban on access to violent video games deemed too violent for those under 18 violates their First Amendment rights).
[40] *Privacy ANPR* at 51282 (questions 14-21).
[41] *See* Section V.
[42] *See* Section V.c.
[43] *Privacy ANPR* at 51284 (question 63).
[44] Virginia State Board of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

regarding the use of prescription drug data.[45] As the Court explained, "[a]n individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way in which the information might be used' or disseminated."[46] But the harm from restricting the use of data affects not just advertisers but also consumers. Customers rely on advertising to find problem-solving products and services they do not know exist, to identify gift ideas for loved ones, and to support their local economy. Receiving truthful advertising is not only helpful for consumers but is also their right. As the U.S. Supreme Court stated in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc*, "[i]f there is a right to advertise, there is a reciprocal right to receive the advertising."[47]

The vast majority of advertising is not false, deceptive, or illegal and therefore receives First Amendment protections. In order for a regulation restricting truthful commercial speech to pass constitutional muster: (1) the government must assert a substantial interest in restricting the speech; (2) the regulation must directly and materially advance that interest; and (3) the regulation must be narrowly tailored to serve that interest.[48] Commercial free speech includes the right of businesses to communicate with consumers without undue hindrance, and courts have struck down previous laws that have banned or overly restricted advertising. For example, in 1999, the Supreme Court unanimously held that a federal ban on advertisements for lawful private casinos was an illegal regulation on commercial free speech.[49] The Court found that the government's ban would not solve the social ills related to gambling that the ban purported to address, and as a result, the ban unreasonably prohibited a specific type of speech.[50] Similarly, the Court struck down Vermont's restrictions on sharing prescriber data because the data restrictions did not advance the state's interest in improved public health or reducing healthcare costs while imposing significant burdens on speech.[51] Similarly, the Commission cannot solve the litany of alleged societal harms enumerated in the Privacy ANPR through broad restrictions on the responsible use of data.

If the FTC seeks to address specific harmful privacy abuses, it should carefully tailor regulation to that end. Any ban or unreasonable limitation on data-driven advertising or other routine and essential practices would be far from narrowly tailored and would not give consumers more information about companies' data practices or combat stalking, mental illness, or discrimination—the ills the Commission states it seeks to address.[52] A blanket ban on data-driven advertising and other uses of data in the marketplace would be the most extreme step the FTC could take to advance its alleged substantial interest and would likely be struck down as an illegal abridgement of bedrock First Amendment protections.

---

[45] Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).
[46] *Id*. at 568 (quoting Seattle Times Co. v. Rhinehart, 467 U. S. 20, 32 (1984)).
[47] 425 US 748, 757 (1976).
[48] Central Hudson Gas & Electric v. Public Svc. Comm'n, 447 U.S. 557, 564 (1980).
[49] Greater New Orleans Broadcasting Ass'n, Inc. v. United States, 527 U.S. 173 (1999).
[50] *Id.* at 189.
[51] Sorrell, 564 U.S. at 572.
[52] *Privacy ANPR* at 51275-76.

c. The major questions doctrine represents a legal challenge to FTC action beyond its congressional mandate.

The extraordinary breadth of consumer privacy issues referenced in the Privacy ANPR suggests that the FTC is considering regulations applicable to the entire U.S. economy. As Commissioner Phillips asserted in his dissent, the ANPR "recast the Commission as a legislature, with virtually limitless rulemaking authority where personal data are concerned."[53] The Commission should be mindful of inevitable court challenges brought under the major questions doctrine based on the Privacy ANPR—particularly given that Congress has not clearly granted the FTC authority to regulate consumer privacy broadly. In fact, Congress's current deliberations over a federal privacy bill show that Congress believes congressional action is required to enable the Commission to do the very work it is attempting to begin now.[54]

The FTC should be cautious about wading into regulating a "major question" without clear congressional direction to do so. The major questions doctrine holds that courts "expect Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance."[55] Regulating the use of data by companies across the entire modern economy and Internet plainly constitutes a major question. Congress's current struggle to negotiate the contours of a federal privacy bill demonstrates the significance of the subject matter and that Congress is where such important debates should be settled.

Given this canon of statutory interpretation, any FTC rulemaking that attempts to define the amorphous term of "commercial surveillance" would be unlikely to receive *Chevron* deference from courts. The "major questions doctrine" holds that courts should not grant *Chevron* deference to agency statutory interpretations that concern questions of "vast economic or political significance."[56] Earlier in 2022, the U.S. Supreme Court invalidated the Environmental Protection Agency's ("EPA") Clean Power Plan as an overreach and misinterpretation of a long-standing yet infrequently used authority.[57] The Supreme Court also noted that the EPA's interpretation of its own mandate "conveniently enabled it to enact a program that, long after the dangers posed by greenhouse gas emissions 'had become well known, Congress considered and rejected' multiple times."[58]

The Privacy ANPR suggests the FTC is preparing to establish a program that Congress has been considering for many years and has yet to approve. Though the Commission may wish to accord broad regulatory power to itself, its attempt to assert such power now, after years of congressional deliberation and lack of final action on federal privacy bills, serves only to confirm that the FTC does not have the power it wishes to wield. As explained by Justice Frankfurter in a case involving FTC overreach: "[J]ust as established practice may shed light on the extent of power conveyed by general statutory language, so the want of assertion of power by those who

---

[53] *Privacy ANPR* at 51294.
[54] H.R. 1892, 117th Cong. (2022).
[55] Utility Air Regulatory Group v. EPA, 573 U.S. 302, 324 (2014).
[56] West Virginia v. EPA, 142 S. Ct. 2587 (2022).
[57] *Id.*
[58] *Id.* at 27 (citing Brown & Williamson, 529 U. S. 120, 144 (2000)).

presumably would be alert to exercise it is equally significant in determining whether such power was actually conferred."[59]

Similarly, in *Alabama Association of Realtors v. Department of Health and Human Services*, the Court held that the Centers for Disease Control and Prevention ("CDC") had exceeded its authority under the Public Health Service Act when it extended a moratorium on evictions.[60] There, the Court blocked this extension of CDC authority, noting the scope of the CDC's claimed authority, the unprecedented nature of the action, and that Congress had declined to extend the moratorium it had previously passed as part of the COVID-19 relief bill.[61] Here, the FTC is asserting unprecedented broad authority to regulate the entirety of the Internet and the data-driven economy, despite Congress repeatedly considering—and ultimately rejecting—many opportunities to pass legislation granting this kind of authority.

One clear example of how the major questions doctrine would limit Commission action based on the Privacy ANPR is in the area of targeted advertising. The Commission has never attempted to regulate or limit this practice in the decades that it has been active in the marketplace, and it even recognized the industry's work to self-regulate based on the principles the Commission produced in leu of regulation.[62] Because Congress has not clearly provided authority for the Commission to regulate in this area and the Commission has never asserted such authority in the past, it is not clear that such authority actual exists within the Commission's toolkit in a manner that would satisfy the Court. For these and the many other reasons carefully described in our comments, the Commission should withdraw and revise the Privacy ANPR to take a more focused approach that is rooted in addressing concrete harms that Congress directed it to address, namely prevalent unfair and deceptive acts and practices.

IV. The FTC's record of enforcement, guidance, and reports fails to provide an adequate record of injury or harm to support rulemaking in many areas that the Commission identifies in the Privacy ANPR.

We believe that the administrative record created by the Privacy ANPR (should it remain open in its current form) deserves a thorough response. However, the Privacy ANPR requests that commentors explain to the Commission, among various other topics, how companies "surveil" consumers, what practices and harms are "prevalent" in the economy, and what categories of data should be regulated and why.[63] The strikingly pejorative assumptions made by the Commission about the use of data by businesses—shown through the Privacy ANPR's use of the negative term "surveillance" —are troubling. Rather, the Commission should enter this process with a neutral and inquiring point of view, building on the long past and present indications of the Commission's recognition that great value exists in the responsible use of data.

---

[59] FTC v. Bunte Bros., Inc., 312 U.S. 349, 352 (1941).
[60] 141 S. Ct. 2485, slip op. at 3 (2021).
[61] *Id.* at 6-8.
[62] FED. TRADE COMM., FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009) (hereinafter *OBA Report*); FED. TRADE COMM., CROSS-DEVICE TRACKING: AN FTC STAFF REPORT (Jan. 2017) (hereinafter *Cross-Device Report*).
[63] *See Privacy ANPR* at 51281 (Questions 1-12).

One need only look at the FTC's decades of work in the data privacy realm to find a far more balanced approach to the important role data plays in the economy. The Commission should, based on its own work, provide a more focused and detailed request for comment in the Privacy ANPR, particularly given that it has repeatedly examined different aspects of the data-driven economy in the past. The Commission's seminal 2012 report on privacy and the use of data by businesses, for example, is not cited once throughout the entire Privacy ANPR.[64] Instead, the Commission lists a series of enforcement actions, news articles, workshops, and reports that purportedly show a need for the present rulemaking process. While some of the practices cited are clearly egregious,[65] the Privacy ANPR does not effectively differentiate these activities from the larger set of responsible, routine, and essential data practices used by the majority of the economy daily to deliver value to consumers and businesses alike. Throughout the Privacy ANPR, the FTC fails to tie specific practices to potential or observed harms, opting instead to speculate and prejudge that certain activity may be considered harmful or injurious "surveillance."

Below we explain that: (1) the FTC is required to constrain its rulemaking considerations to address concrete and cognizable harms and to how to identify those harms; (2) many routine and essential data practices are not harmful and should be out of scope for the Commission's process; (3) there is a lack of history of harm related to data-driven personalization and third-party data activity; (4) transparency and choice are important in preventing consumer injury and deception, including related to "dark patterns"; and (5) the FTC lacks authority to step into employee-employer and similar relationships.

a. The FTC must use a concrete and cognizable standard for harm to address injuries within its enforcement purview.

The FTC must be specific when describing harms it seeks to prevent through the rulemaking process, and the scope of such harms is limited by the FTC's statutory grant of authority and constitutional requirements. The FTC is constrained by the FTC Act to issuing trade regulations for unfair or deceptive acts and practices, and to do so, the FTC must determine that an act or practice "cause[s] or [is] likely to cause reasonably foreseeable injury."[66] Given the open-ended nature of the Commission's inquiry, it is unlikely that many data practices that would be included within its definition of "commercial surveillance" will meet the standard of injury necessary for the FTC to declare them unfair or deceptive. The Commission should examine and seriously consider how it will define the harms it proposes to address through the rulemaking and whether these harms and associated acts or practices would meet the requirements of the FTC Act.

Congress and the FTC have further defined unfair and deceptive practices through statutory amendments and policy statements, recognizing that the Commission must focus on

[64] FED. TRADE COMM., PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (hereinafter *2012 Report*).
[65] *See Privacy ANPR* at 51278 (regarding *In re Craig Brittain* and *FTC and State of Nevada v. EMP Media, Inc.*, "solicitation and online publication of 'revenge porn'—intimate pictures and videos of ex-partners, along with their personal information—and the collection of fees to take down such information").
[66] 15 U.S.C. § 45(a)(4)(A)(i).

substantial injury when exercising its power to declare an act unfair.[67] This focus lies behind the Commission's questions seeking to understand what types of injury and harm its rulemaking should address.[68] Regardless of the type of specific harm the FTC seeks to address, the FTC's question must first be whether the potential injury is concrete or real and not "abstract" or "hypothetical" such that it would fail Article III standing standards.[69]

The most typical and concrete injuries the FTC may address are tangible and measurable through objective means. Monetary injury is the exemplary injury the Commission primarily seeks to prevent and redress.[70] The FTC has a long history of prosecuting unfair practices that result in monetary harm to consumers, such as when companies facilitate fraud.[71] The loss of money represents a clear and redressable harm to consumers that, if the Commission found a practice was prevalent and unfair resulting in wide spread monetary injury to consumers, would be ripe for rulemaking.[72] A more limited type of injury the Commission could seek to prevent is physical injury or safety. For instance, where data about consumers may be used to stalk or assault individuals, the Commission may use its authority to prevent that harm.[73] However, even this type of physical injury must not be hypothetical but instead based on facts that indicate a likelihood, not a mere possibility, of harm.[74]

Another form of injury on which the Commission appears to focus in the Privacy ANPR includes intangible injury, such as reputational or psychological harm.[75] While the Commission has recognized that such harms are possible, it noted that they will "not ordinarily make a practice unfair."[76] The Commission has not, however, delineated when and how such harms could support a finding of unfairness in the Privacy ANPR. In fact, Congress made clear that the Commission may not rely on "public policy" as the primary basis for determining an act is unfair.[77] Because the Commission must show an identified likelihood of harm resulting from a practice, and not primarily a desire for a public policy outcome, the Commission must rely on more than media reports that certain intangible harms "may" result from a particular practice and

---

[67] *Id*. § 45(n); FED. TRADE COMM., POLICY STATEMENT ON DECEPTION (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf; FED. TRADE COMM., FTC POLICY STATEMENT ON UNFAIRNESS (Dec. 17, 1980) (appended to *Int'l Harvester Co*., 104 F.T.C. 949, 1075 (1984)), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness. (hereinafter *Unfairness Policy Statement*) ("[T]he focus on injury is the best way to ensure that the Commission acts responsibly and uses its resources wisely.").

[68] *Privacy ANPR* at 51281 (questions 4-10).

[69] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2018) (describing the requirement for "concrete injury" to satisfy Article III standing); Beals, Kim, et. al., CONSIDERATIONS FOR FRAMING, ASSESSING, AND BALANCING ACTIONABLE INJURY AND INTANGIBLE HARM RELATING TO PRIVACY AND DATA PROTECTION, 4 (2018).

[70] The FTC recognized this in its 1980 Unfairness Policy Statement noting that "*in most cases* a substantial injury involves monetary harm." *Unfairness Policy Statement* at 1073 (emphasis added).

[71] Complaint, FTC v. Blue Global & Christopher Kay, F.T.C. File No. 2:17–cv–02117 (D. Ariz. July 3, 2017).

[72] This is just the type of activity and injury the Commission is currently seeking to regulate in its open rulemaking process regarding government and business impersonation.

[73] *See e.g.,* Complaint, In re Trendnet, Inc., F.T.C. File No. 122-3090(Feb. 7, 2014) (alleging security flaws in Internet security camera increase risk that consumers will be targeted for criminal activity).

[74] FTC v. D-Link Corp., F.T.C. File No. 3:17-CV-00039-JD, 2017 WL 4150873, at *5 (N.D. Cal. Sept. 19, 2017).

[75] *Privacy ANPR* at 51281 (question 9).

[76] *Unfairness Policy Statement* at 1073.

[77] 15 U.S.C. § 45(n); S. Rep. No. 103-130, 1993 WL 322671, at *13 (F.T.C. Aug. 24, 1993) ("Emotional impact and more subjective types of harm alone are not intended to make an injury unfair.").

general statements that consumers feel they must "surrender" information to engage in certain daily activities.[78] A Privacy ANPR that identifies specific harms the Commission desires to address through Mag-Moss rulemaking could help establish a record to aid in this judgement, but the FTC did not issue such a document here.

b. Routine and essential data practices should be outside the FTC's consideration given the lack of proven harms.

In the Privacy ANPR, the Commission broadly asks what practices are used to "surveil" consumers, but its definition of "commercial surveillance" includes virtually any data processing activity used to operate a business.[79] One limiting principle that can help focus the FTC's considerations is that the routine and essential data practices used to support the data-driven economy represent the vast majority of data processing activities within the Commission's scope. Such practices should be considered *per se* reasonable and outside the purview of the rulemaking process.[80] These practices do not represent widespread, prevalent sources of injury and are necessary for consumers to engage with and receive the various benefits provided by the data-driven economy. In fact, these activities are key to innovation and continued economic development that data supports.[81]

Privacy for America, for example, examined which activities represent these necessary data practices, and defined them to include:

> [T]he lawful collection and use of personal information only as reasonably necessary to: (1) respond to valid legal process or as required or specifically authorized by law; (2) protect public safety; (3) provide security for a product or service; (4) prevent and detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or take action against those responsible; (5) authenticate and verify the identity of an individual exercising one or more of the choices required under this law; or (6) provide an individual with notice of product recalls.[82]

Additionally, Privacy for America determined that customer communications,[83] fulfillment,[84] and marketing research[85] were activities that, when conducted legally,

---

[78] *See Privacy ANPR* at 51273.
[79] *Privacy ANPR* at 51281 (question 1).
[80] A similar conclusion was found by the Commission in its 2012 Privacy Report. *See 2012 Report*.
[81] *Privacy ANPR* at 51282 (question 26 & 29).
[82] *Privacy for America* Part I, Section 1(Y).
[83] Defined as communicating "with an individual with whom the covered organization has a customer relationship, including for the purposes of providing support for a product or service, or providing advertising and marketing communications about the covered organization's new or existing products or services." *Privacy for America* Part I, Section 1(J).
[84] Defined as "the collection, use, maintenance, or transfer of personal information only as reasonably necessary to: (1) Deliver or provision a product or service requested by the individual to whom the information relates; or (2) Conduct administrative activities routinely associated with and necessary to perform the activity in Subsection (1), such as billing, shipping, and accounting." *Privacy for America* Part I, Section 1(O).
[85] Defined as "the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (1) integrated

should not be restricted by most of the Privacy for America *Framework*'s prohibitions on unreasonable activity.[86] The Commission should take a similar approach and make clear that certain beneficial and routine activity—when done legally—is not unfair or deceptive.

The 117th Congress is considering an approach that adopts parts of the *Framework*. The proposed American Data Privacy and Protection Act ("ADPPA") defines a set of permissible purposes for data collection that include many of the Privacy for America *Framework*'s defined practices.[87] While we disagree with many of the operative standards of the ADPPA and its underinclusive list of permissible purposes, the proposed legislation reveals that Congress is identifying data processing activities that are reasonable and should not be limited by a regulatory framework for data privacy. This suggests that the FTC should follow a similar path by identifying the limited, specific, practices that can meet the stringent definitions of prevalent unfair or deceptive acts or practices and therefore justify regulatory limits on such activity.

c. "Targeted advertising" and other content personalization products and services do not create *per se* cognizable "harms" and have long been recognized by the FTC as reasonable practices.

The Commission asks several questions about potential harms or impacts of banning (or limiting) aspects of the data-driven economy associated with personalization.[88] We discuss below the myriad benefits provided to consumers by personalization of advertising and other interactions facilitated through data.[89] In addition, the Commission has not traditionally found that these activities represent unfair or deceptive acts and practices. In fact, the Commission has often recognized that such activity, when engaged in responsibly, delivers great benefits to consumers and the FTC has worked with the business community to help establish how that responsible data processing activity can occur.[90] Given the lack of real concrete harm related to personalization and targeted advertising, such practices are not appropriate grounds for Commission regulation.

Indeed, the limited cases the Commission cites in the Privacy ANPR do not stand for the proposition that personalization and targeted advertising represent unfair or deceptive practices. These cases instead are directed at correcting various alleged specific misrepresentations or other allegedly deceptive activity related to data collection and use practices.[91] Whether companies are alleged to have ineffective opt-out mechanisms or misrepresentative notices to consumers, the Commission has focused on the deceptive nature of those specific actions rather than on the

---

into any product or service; (2) otherwise used to contact any particular individual or device; or (3) used to advertise or market to any particular individual or device." *Privacy for America* Part I, Section 1(R).

[86] *Id*. at Part I, Section 3(O).

[87] H.R. 8152, Section 101(b).

[88] *Privacy ANPR* at 51283 (question 39-42); 51284 (question 62).

[89] *See* Section V.

[90] *See e.g., OBA Report*; *2012 Report*; *FED. TRADE COMM., DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY,* v (2014); *FED. TRADE COMM*, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?, i (2016); FTC, *Cross-Device Report*, 5-6.

[91] *Privacy ANPR* at 51278-79.

underlying data practice itself.[92] Even when the Commission has alleged that unfair practices have taken place with regard to targeted advertising, it has based this finding on the alleged sensitivity of the data in question—not on the practice of collecting data to personalize advertising or other services.[93] Nothing in the FTC's record of enforcement supports a finding that targeted advertising or data-driven personalization are prevalent unfair or deceptive practices within the meaning of the FTC Act.[94]

Against this backdrop, the Commission's use of pejorative terms such as "commercial surveillance" to address such practices is unexpected, especially given the FTC's history of support for using data to deliver personalized content and advertising discussed above. The Commission should base any attempts at regulating these economically and socially valuable practices on clear evidence, and not on a desire by the Commission today to effectuate a public policy banning or severely limiting those practices. We address the immense value and benefits of targeted advertising and data-driven personalization in Section V.

d. Data services companies, third-party data, and derived data are valuable and essential parts of an efficient and competitive marketplace.

The Privacy ANPR seeks comment on whether data practices should be limited to providing only the services requested by a consumer and whether the Commission should limit the ability to use and transfer data to other entities and for purposes other than for which the data may have been previously collected.[95] Such restrictions appear to be focused, at least in part, on the third-party data industry and the ability to use data collected for one purpose for derivative purposes. Once again, the FTC's enforcement history does not support drastic limitations on third-party and derivative data practices or to label such practices as prevalent unfair or deceptive practices.

The Commission has obtained settlements with companies for various data sharing practices and the use of data for purposes other than the stated purpose for which it was initially collected.[96] These cases, however, once again point to alleged misrepresentations specific to the facts of the respective cases, not to any specific underlying data practice that is prevalent in the marketplace that results in substantial injuries to consumers. These cases convey that companies should honor their stated commitments to consumers—a bedrock of privacy law—and the FTC's history of deception enforcement.

In the past, when the Commission has discussed third-party data, the companies that supply that data, and the use of data for derivative purposes, it has recognized the various

[92] *See e.g.,* Complaint, In re Turn Inc., F.T.C. File No. 152–3099 (Apr. 6, 2017); In re MoviePass, Inc., F.T.C. File No. 192–3000 (Oct. 1, 2021).
[93] Complaint, FTC v. Vizio, Inc., F.T.C. Case No. 2:17-cv-00758 (D.N.J. Feb 6, 2017) (alleging that television viewing data is particularly "sensitive" and therefore its collection in an allegedly surreptitious manner was injurious enough to be unfair) (hereinafter *Vizio*). We do not endorse the Commission's allegation that television viewing information is, by itself, sensitive in nature.
[94] Similar sentiment was highlighted by Commissioner Phillips in his dissenting statement. *Privacy ANPR* at 51295.
[95] *Privacy ANPR* at 51283 (questions 43-46).
[96] *See e.g.,* FTC, In the matter of Flo Health, Inc., FTC File No. 1923133 (2021) (hereinafter *Flo Health*); United States v. Twitter, Inc., F.T.C. Case No. 3:22– cv–3070 (N.D. Cal. May 25, 2022).

benefits they provide to competition and consumers.[97] Furthermore, when the Commission has discussed the potential risks related to third-party data practices, those risks have been speculative in nature (such as an insurance company possibly using data from searches for premium setting), which fails to meet the standards for cognizable injuries discussed above.[98] Even if these risks were to become real, the benefits (*e.g.*, risk mitigation, fraud prevention, and efficient marketing, among others) provided by the third party data ecosystem far outweigh the limited actionable harm that could theoretically impact some consumers.[99] The FTC Act does not authorize the Commission to broadly regulate this segment of the data-driven economy.

Furthermore, regarding derived and inferred data (which the Commission includes in its definition of "commercial surveillance"), the FTC should be circumspect in interfering with these data operations that businesses perform on their own data to provide the types of valuable and beneficial services third-party data companies offer.[100] Derived data is data generated by the business itself through its own proprietary and often trade secret-protected processes. This data is not collected from a consumer. While derived data may be associated with a consumer for a variety of purposes, such as to deliver relevant advertising or prevent payment fraud, its nature as derived or inferred data does not present an inherent risk of harm or injury that should be addressed by the Commission.[101] The Commission should instead focus on specific data practices that can be defined as prevalent deceptive or unfair acts or practices, not on any and all data that might be used in the marketplace.

e. Transparency and choice continue to play a significant and meaningful role in the data-driven economy and serve as a bedrock of consumer privacy.

By proposing to issue regulations that would limit the ability of consumers to provide consent to companies for certain data practices, the Commission appears interested in overturning policy developed over decades.[102] The Commission indicates that its dim view of consent is a result of the "reported scale, opacity, and pervasiveness" of "commercial surveillance."[103] The FTC specifically cites uses of "dark patterns" as examples of how it says consumer consent and transparency may no longer provide protections in the marketplace.[104] These general statements and appeals to current public policy debates do not, however, help identify practices that represent unfair or deceptive acts that are prevalent and ripe for regulation.

---

[97] *See 2012 Report* at 43-44 (recognizing that third party data enhancement is a legitimate and useful practice in the marketplace); FED. TRADE COMM., DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 47-48 (2014) (recognizing the benefits of data brokers); FED. TRADE COMM, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 5-7 (2016) (recognizing the benefits of big data and derivative uses of data).
[98] *See* Section V.b.
[99] *See* Section V.
[100] *Privacy ANPR* at 51277.
[101] These benefits are further discussed in Section V.
[102] *Privacy ANPR* at 51284 (questions 73-82). Additionally, as discussed in Section III, consumers have a First Amendment right to receive advertising and other commercial speech, especially when they request that speech be delivered to them.
[103] *Id*. (question 73).
[104] *Privacy ANPR* at 51280; 51287.

The Commission has long held that effective, truthful, and clear notice to consumers is vital for an effective data privacy regime.[105] Based on this history of guidance and engagement, the digital advertising industry created the Digital Advertising Alliance ("DAA") to implement the enhanced transparency and clear, meaningful, and effective consumer choice suggestions the Commission outlined in its reports.[106] The DAA's YourAdChoices Icon is recognized by 82% of consumers, who indicate that they understand that the Icon signals data-driven advertising is present along with their content. The majority of these consumers further convey that they understand that they can use that icon to access information about data privacy choices.[107] Far from being irrelevant to many data practices, such effective approaches to enhanced transparency are integral to increased consumer protection and understanding about how data benefits them in the marketplace.

The Commission has recognized this work and the self-regulatory programs the Commission fostered as increasing the level of consumer protection in the marketplace.[108] Indeed, the FTC should continue to encourage effective, clear, and meaningful notices for consumers as a means of mitigating potential harms that may stem from deceptive omissions or statements as well as from potentially unfair data practices. The logic of this approach is shown in the Commission's own enforcement in which the Commission often requires providing such notices to consumers as a remedy for alleged unfair or deceptive data practices.[109]

So-called "dark patterns," a term the Commission uses to encompass another broad set of alleged misconduct, represents another example of alleged shortcomings in effective transparency and choice that the Commission can effectively police through existing Section 5 authority. The Commission's recent report on the topic refers to cases alleging that "dark patterns" include deceptive omissions or design elements that either prevent effective notice from reaching consumers or make outright misrepresentations to consumers.[110] The Commission identifies in its report cases that allege fraud by presenting misleading association with the U.S. military, basic deception issues such as abridged statements or confusing interfaces, and alleged violations of the Restore Online Shoppers Confidence Act ("ROSCA") as the Commission's examples of "dark patterns."[111] These identified cases are already capable of being addressed by the Commission's existing authority. Additionally, in the case of alleged ROSCA violations, the FTC has enhanced ability to respond to violations through authority granted by Congress to address new online data and business practices. The extreme breadth of practices that the Commission includes within its definition of "dark patterns" makes it

---

[105] *See OBA Report* at 33-37; *2012 Report* at 61-63; *Cross-Device Report* at 11-15.
[106] *See OBA Report*; DAA, www.youradchoices.com (2022).
[107] DAA, AdChoices: The World's Gateway To Privacy Information 1 (2021), https://digitaladvertisingalliance.org/icon_assets/DAA_2021_AdChoices_Icon_Awareness_Survey.pdf.
[108] "FTC staff commends these self-regulatory efforts to improve transparency and choice in the cross-device tracking space. Both the NAI and DAA have taken steps to keep up with evolving technologies and provide important guidance to their members and the public. Their work has improved the level of consumer protection in the marketplace." *Cross-Device Report* at 11.
[109] *See e.g., Vizio,* Order; *Flo Health,* Order.
[110] Fed. Trade Comm., Bringing Dark Patterns to Light (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.
[111] *Id*.

extremely difficult for the Commission to produce specific, actionable regulations through this current rulemaking process.

Additionally, consumer choice represents a foundational principle of the U.S. economy, and when effective and informed choice is possible, the FTC should not substitute its determination about how consumers choose to engage with businesses.[112] The type of public policy-based outcome that the Commission appears to be driving towards is exactly the type of activity that led Congress to limit the Commission's rulemaking authority and codify the unfairness and deception principles in law. Before the FTC takes another leap into regulating everyday interactions between consumers and businesses and removing valuable choice from the marketplace based on the current Commission's opinion of what a consumer may engage in "for their own good," the FTC should assess such actions against the objective standards for deception and unfairness (including the need for a showing of prevalence and an addressable concrete injury).

f. The FTC has a limited history of regulating business-to-business, employee-employer, and franchisee-franchisor relationships in its consumer protection mission and should not stray into such areas without clear authority.

The Commission cites a limited number of cases to argue that the Privacy ANPR's definition of "consumer" should include business-to-business and employee-related data.[113] However, the cases cited focus on data security breaches that impacted worker-related data and deceptive claims where businesses purportedly failed to meet their public commitments to their workers.[114] The relationships between worker and employer and between sophisticated businesses are highly regulated in many states and negotiated between the parties. Additionally, business-related credit reports are vital to effective capital markets and business transactions and fall outside of the consumer-focused Fair Credit Reporting Act. Applying the same rules and regulations to these relationships is not reasonable and would cause unintended consequences for both businesses and employees as well as employees' potential ability to engage in work.

---

[112] *See Privacy ANPR* at 51296; J. Howard Beales III & Timothy J. Muris, *Return of the National Nanny*, WALL STREET J. (May 26, 2022), https://www.wsj.com/articles/return-of-the-national-nanny-ftc-activists-rulemaking-regulation-banning-mandates-illegal-11653596958.

[113] *Privacy ANPR* at 51277.

[114] *See, e.g.,* Press Release, Fed. Trade Comm'n, *FTC Settles Charges Against Two Companies That Allegedly Failed to Protect Sensitive Employee Data* (May 3, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed-protect-sensitive-employee-data; Press Release, Fed. Trade Comm'n, *Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees* (July 27, 2010), https://www.ftc.gov/news-events/news/press-releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-financial-privacy-customers-employees; Press Release, Fed. Trade Comm'n, *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations* (Feb. 18, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial-privacy-customers-employeescvs. *See also* Press Release, Fed. Trade Comm'n, *Amazon To Pay $61.7 Million to Settle FTC Charges It Withheld Some Customer Tips from Amazon Flex Drivers* (Feb. 2, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/02/amazon-pay-617-million-settle-ftc-charges-it-withheld-some-customer-tips-amazon-flex-drivers.

Given the unique nature of these relationships and the role of business and employee data in a variety of regulatory and financial requirements, the Commission should reconsider regulations in this space. The Commission has already taken a broad approach to the traditionally understood consumer data ecosystem, and the addition of business-related data to that portfolio is the wrong approach to achieve the stated goal of creating rules to protect what are traditionally understood to be "consumers."

V. The value of data to consumers and the economy should not be diminished by overbroad and restrictive rules.

Mag-Moss rulemaking requires the FTC to perform a cost-benefit analysis of its potential rulemaking actions to develop an administrative record that is supported by "substantial evidence" and thus less prone to being overturned on judicial review.[115] While the Privacy ANPR provides a laundry list of alleged, theoretical harms associated with "commercial surveillance,"[116] it fails to give due consideration to the tremendous value the use of data offers individuals and the economy alike. Data is the key that has unlocked massive strides in economic development and human potential. Removing data from the economy or severely limiting its responsible use via regulation would impede firms and institutions from continuing to leverage data to improve Americans' lives. A regulation severely limiting the ability to harness the power of data would impose far more costs on individuals and businesses than theoretical benefits that would derive from mis-calibrated rules.

Myriad benefits accrue from the responsible use of data. Data powers U.S. innovation and facilitates improved decision-making, which helps create timely, critical advancements across industries. Data also unleashes economic growth by driving rises in gross domestic product ("GDP"), creating new high-value employment opportunities for individuals, and helping consumers find useful products and services that enrich their lives when those products and services are most relevant to the consumer. Moreover, data supports individuals' ability to access a wealth of information for free or next to no cost, and it enables a vibrant marketplace of businesses of all sizes to compete and drive each other to deliver ever-improving products and services to consumers. Data powers critical discoveries and tools that have been estimated to generate trillions of dollars in value each year in the United States.[117] The Privacy ANPR gives no consideration to these benefits or other significant advantages that accrue from the use of data by businesses. Failing to consider the vast benefits that the use of data offers society will result

---

[115] 18 U.S.C. § 57a(e)(3).

[116] *See, e.g., Privacy ANPR* at 51274 ("Most consumers... know little about… consumer profiles that can expose intimate details about their lives and, in the wrong hands… expose unsuspecting people to future harm."), 51275 ("The material harms of these commercial surveillance practices… may increase the risks of cyber attack by hackers, data thieves, and other bad actors…. Companies' collection and use of data have significant consequences for consumers' wallets, safety, and mental health.").

[117] JAMES MANYIKA ET AL., OPEN DATA: UNLOCKING INNOVATION AND PERFORMANCE WITH LIQUID INFORMATION, McKinsey Global Institute 6 (Oct. 2013), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information. These benefits derive from myriad sources, such as increased price transparency creating lower prices for consumers, better product discovery spurring innovation, and more efficient transactions removing fraud and waste to benefit consumers and businesses alike.

in a regulatory record devoid of imperative information needed to guide the generation of meaningful and well-considered regulations.

Without giving appropriate and honest weight to the clear and significant benefits the responsible use of data has bestowed on U.S. society, numerous routine and accepted data practices that bring consumers daily value could be swept in by overbroad regulations that seek to address supposed "harms" associated with uses of data. The FTC should scrutinize its assumptions regarding consumer harm, and how it attempts to define such harms, against the various benefits described herein. A regulation unreasonably constricting the ability to use data in the name of protecting consumers from an amorphous concept of "commercial surveillance" could remove critical opportunities for continued advancement and growth.

While we provide the studies and information below, we urge the Commission to reassess its ability to conduct research and economic analysis itself to better understand the marketplace and inform a revised Privacy ANPR in the future. This type of careful economic study and analysis is something that regulators in Europe, the United Kingdom, Australia, and other countries have taken great effort to perform *before* issuing or creating regulatory frameworks that could threaten the economic benefits of data. The benefits of data, as discussed in more detail below, must be an integral input for the Commission's consideration if it proceeds with Mag-Moss rulemaking.

a. Data supports the economy and adds significant value to individuals' lives.

The Privacy ANPR suggests that collection and use of data has exposed individuals to a host of physical, mental, and financial harms.[118] While the Privacy ANPR lists numerous examples of alleged harms, it fails to concretely connect those harms to the general availability of data in the marketplace.[119] By providing a list of attenuated harms without attributing them to present specific uses of information that require attention, the FTC obscures the issues it is attempting to address through rulemaking. Moreover, the Privacy ANPR does not consider or even mention that the responsible use of data in the marketplace is the bedrock of the modern economy, delivering free and low-cost services to consumers and creating jobs across the country. In fact, documents supporting the Privacy ANPR lambast the idea that companies should be able to derive economic value from data at all.[120] The FTC incongruously appears to criticize companies' ability to use data to make money by creating better products and services, and marketing those products and services, to deliver societal benefits.[121]

The Privacy ANPR asks: "What are the benefits or costs of refraining from promulgating new rules on commercial surveillance or data security?"[122] A key benefit of refraining from

---

[118] *Privacy ANPR* at 51275.
[119] As discussed in Section IV.
[120] FED. TRADE COMM., FACT SHEET ON THE FTC'S COMMERCIAL SURVEILLANCE AND DATA SECURITY RULEMAKING at 1, https://www.ftc.gov/system/files/ftc_gov/pdf/Commercial%20Surveillance%20and%20Data%20Security%20Rulemaking%20Fact%20Sheet_1.pdf ("Companies may use some of the information they collect to provide products and services, but they can also use it to make money.").
[121] *Id*.
[122] *Privacy ANPR* at 51282 (question 29).

promulgating new rules would be to maintain the present value and efficiency of the economy. The entire marketplace—companies and individuals alike—benefit from the responsible use of data.

i. Data use contributes significantly to U.S. GDP and consumers' livelihoods.

The use of data has been a catalyst for significant economic growth in the United States. Data use drives an overwhelming and consistently growing portion of U.S. GDP every year.[123] The responsible use of data has allowed the U.S. to become an economic leader across various industries and to deliver untold benefits to society. The data economy also generates millions of jobs for individuals. In 2020, more than 17 million people in the U.S. were employed in jobs generated by the free flow of data.[124] Of those jobs, more were created by small firms and the self-employed (38%) than by the largest firms (34%).[125] Data thus contributes significantly to the overall economic output of the United States and helps to enrich the lives of individuals by providing opportunities for high-value employment. The U.S. data-driven marketing and advertising-supported economy is a growth and jobs catalyst for the entire U.S. economy. The FTC must account for any harms its potential regulations would inflict on that engine.

In addition, businesses' applications and uses of data improve consumers' lives by providing them with tools and protections that facilitate their safe engagement with the economy. The FTC's cost-benefit analysis must reflect the extensive value that secondary uses of information—*i.e.*, uses of information that are unrelated to the original purpose for which the information was collected—can provide to individuals and the economy. For example, several fraud detection and control tools use data originally collected for a different purpose to discover and prevent unauthorized uses of personal information. This use of data helps banks and other financial institutions detect and stop fraudulent purchases with credit cards often before the cardholder even learns about such activity.[126] Data also allows the healthcare industry to mitigate fraud and abuse by stopping illegal billing for falsified medical claims, detecting false claims filed by multiple providers, and limiting the incidents of stolen patient identities to gain reimbursement for medical services that were never provided.[127] Fraud prevention is just one example of various ways businesses have harnessed the power of data to deliver benefits to consumers and society at large when the data in question was first collected for other purposes. The promotion of safe and efficient transactions, e-commerce, and digital activity is one of the prime uses of data for derivative purposes and is one of the key factors in the world-leading U.S. digital economy. Unreasonable restraints on permissible uses of data by companies will stop these important consumer protections from efficiently operating.

---

[123] *See* JOHN DEIGHTON & LEORA KORNFELD, THE ECONOMIC IMPACT OF THE MARKET-MAKING INTERNET 5, IAB (Oct. 18, 2021), https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf.
[124] *Id*.
[125] *Id*. at 6.
[126] *See, e.g.,* M. Sathyapriya & Dr. V. Thiagarasu, *Big Data Analytics Techniques for Credit Card Fraud Detection: A Review*, 6 INT'L J. OF SCIENCE & RSCH 206, (2017), https://www.ijsr.net/archive/v6i5/ART20173111.pdf.
[127] *See, e.g.,* P. TRAVAILLE ET AL., ELECTRONIC FRAUD DETECTION IN THE U.S. MEDICAID HEALTHCARE PROGRAM: LESSONS LEARNED FROM OTHER INDUSTRIES (2011).

ii. Data permits access to resources for free or at a very low cost.

In addition to the contributions of data to U.S. GDP, employment, and various data-driven products and services, it is critical for the FTC to recognize that consumer value derived from data may be intangible or an indirect driver of value. Studies have found, for example, that digital goods like access to online search engines and encyclopedias generate a large amount of consumer welfare and value that is currently not captured in U.S. GDP.[128] For instance, data permits consumers to access the powerful tool that is the Internet and its countless products and services for free or at a very low cost. The benefits that free access to the Internet provides to Americans cannot be overstated.

Due in large part to responsible open flows of data across the Internet, consumers can reach resources, content, news, education, videos, music, art, and more without encountering many hurdles or barriers. Because such access is largely free, consumers of all economic backgrounds can reach educational and useful content. Data has consequently helped to level the playing field in terms of individuals' access to informational resources and learning, and it has facilitated the growth of an egalitarian Internet where knowledge is not gatekept behind paywalls or other significant barricades to access. The Privacy ANPR does not address, contemplate, or ask a single question about the cost to society that would result from a loss of open access to the Internet or the implications of losing such access to resources. The significant value provided by the use of data to monetize content efficiently by supporting consumers' access to virtually limitless vital and enriching information will be lost by restrictive regulations that unreasonably limit data collection or use.

iii. Consumers prefer and actively choose the ad-supported model of the Internet.

When consumers do not want data about them to be used to deliver more personalized experiences to enjoy a more accessible and relevant Internet ecosystem, that small subset of consumers can opt out of such data use.[129] Regrettably, the Privacy ANPR ignores this fact. The Privacy ANPR states, "as networked devices and online services become essential to navigating daily life, consumers may have little choice but to accept the terms that firms offer."[130] With regard to targeted messaging on the Internet, this statement is plainly untrue as consumers do have a choice to opt out of such messaging.

The Privacy ANPR suggests that because free online services are essential, consumers are forced to figuratively "pay" for such services by trading their privacy.[131] However, the Privacy ANPR ignores the fact that consumers have weighed the costs and benefits of this tradeoff between data use and access to information, and they have proclaimed that they value

---

[128] ERIK BRYNJOLFSSON ET AL., USING MASSIVE ONLINE CHOICE EXPERIMENTS TO MEASURE CHANGES IN WELL-BEING (Apr. 9, 2019), https://www.pnas.org/doi/10.1073/pnas.1815663116.
[129] DAA, YourAdChoices, https://youradchoices.com/.
[130] *Privacy ANPR* at 51274.
[131] *See id.*; *see also 2012 Report*.

free and low-cost access to information, content, and services to a very high degree.[132] The Commission itself has acknowledged that consumers should be able to decide for themselves whether they want access to data supported products, services, and content. In its 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change,* the FTC stated:

> With respect to less important products and services in markets with sufficient alternatives, take-it-or-leave-it choice can be acceptable, provided that the terms of the exchange are transparent and fairly disclosed – *e.g.*, "we provide you with free content in exchange for collecting information about the websites you visit and using it to market products to you." Under the proper circumstances, such choice options may result in lower prices or other consumer benefits, as companies develop new and competing ways of monetizing their business models.[133]

The Privacy ANPR does not address the FTC's prior approval of consumers' ability to evaluate the tradeoffs between free and open data use and access to online content. Instead of tackling this claim and others in the 2012 report directly, the Privacy ANPR ignores the existence of that watershed document and the benefits of data use outlined in the report. The Privacy ANPR thus ignores many important prior conclusions made by the FTC itself that counsel against unreasonably limiting data processing activity. The Privacy ANPR also appears to suggest that the FTC's calculation of tradeoffs between access to online content and open use of data should be substituted for the decisions of consumers. By substituting its value judgments and viewpoints for the reasoned calculations of consumers themselves, the FTC may indeed revive its reputation as America's "national nanny."[134]

Studies show that the vast majority of consumers value the free nature of the Internet and prefer the ad-supported model, where most content is free, to a non-ad supported Internet where they would be required to pay to reach most content.[135] For example, in a recent survey conducted by the DAA, 90 percent of surveyed consumers stated that free content and information was important to the overall value of the Internet.[136] In that same survey, 85 percent of respondents stated they prefer the ad-supported model of the Internet to a non-ad supported Internet rife with paywalls and other walled garden content.[137] Consumers assign their ability to access the Internet for free or at a low cost an approximate value of over $1,400 per year.[138] Additional research has found that the 2017 value of the goods and services that consumers

---

[132] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 31 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.
[133] *2012 Report* at 52.
[134] *See* WASH. POST, *The FTC as National Nanny* (Mar. 1, 1978), https://www.washingtonpost.com/archive/politics/1978/03/01/the-ftc-as-national-nanny/69f778f5-8407-4df0-b0e9-7f1f8e826b3b/.
[135] DAA, *Americans Value Free Ad-Supported Online Services at $1,400/Year; Annual Value Jumps More Than $200 Since 2016* (Sept. 28, 2020), https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200.
[136] *Id*.
[137] *Id.*
[138] *Id*.

receive through the ad supported Internet to be nearly $30,000 per year.[139] In the Privacy ANPR, the Commission "invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices."[140] Consumers understand the value proposition of ad-supported, data-driven models and actively choose data-driven practices in exchange for myriad benefits. The Commission should not override consumers' ability to choose ad-supported, data-driven content and messaging.

Unreasonable limits on data use through new data regulations would cause many online content and service providers to adopt a subscription-based model, where outlets require payment before content or services may be accessed. This result would be in direct opposition to the stated preference of consumers to maintain the current ad-supported model rather than move to a pay-to-play environment where an increasing amount of content is behind paywalls and other barriers to access. In contrast to this effort to increase opportunities for consumers to exercise granular choices, the Privacy ANPR suggests the FTC may issue broad regulations that would block consumers' ability to receive relevant ads altogether. Overly restrictive limitations on the flow of data would harm consumers more than they would benefit them and would harm those unable to pay for content disproportionately more than those with enough income to replace formerly ad-supported services.

iv. Data-driven messaging provides benefits to society.

Using the power of data to personalize messaging has real and tangible benefits for individuals and society. Companies, nonprofits, and government agencies all use data to address specific messaging to various groups of individuals. Responsible uses of data to target messaging create immense public benefit by reaching individual consumers with information that is relevant to them in the right time and place. Legal requirements that limit entities' ability to use data to reach individuals with important, pertinent, and truthful messaging can have unintended consequences and, ultimately, serve as a detriment to their health and welfare.

Examples of the use of data to improve individuals' lives are everywhere. Targeted messaging is used, for instance, to disseminate Amber Alerts to people in areas where a missing child was last seen.[141] Personalized messaging also enables wildfire warnings to be sent to individuals who are likely to come across the path of an uncontrolled blaze.[142] Even the federal government uses targeted messaging to increase individuals' engagement with offerings that can benefit them. For example, the Department of Health and Human Services ("HHS") used targeted advertising to reach certain communities with tailored information about COVID-19 vaccines in ways that were relevant and meaningful to them. Reports note that HHS "targeted ads to [social media] users interested in 'Native American culture' that featured a woman wearing a mask decorated with Native American symbols and a pledge to 'do my part for all our

[139] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.
[140] *Privacy ANPR* at 51284 (question 73).
[141] Lou Mastria, *Summit Snapshot: Data 4 Good – The Ad Council, Federation for Internet Alerts Deploy Data for Vital Public Safety Initiatives,* DAA (Sept. 1, 2021), https://digitaladvertisingalliance.org/blog/summit-snapshot-data-4-good-%E2%80%93-ad-council-federation-internet-alerts-deploy-data-vital-public.
[142] *Id.*

people.'"[143] This kind of tailored communication has real impact, as it better encourages individuals to engage with the offered product or service in a relevant way.

v. Contextual advertising cannot replicate the benefits of targeted messaging.

The Privacy ANPR includes questions about "alternative advertising practices" companies could "turn to" in the event new rules "limit first- or third-party targeting."[144] Specifically, the Commission asks about contextual advertising and how "cost-effective" it is "as compared to targeted advertising."[145] Forcing the economy away from personalized messaging and data-driven methods of driving engagement, such as targeted advertising, would eliminate significant value and benefits that could not be replicated by other methods. Alternative methods of reaching consumers, like contextual advertising, can serve as helpful additions in this ecosystem. Contextual advertising, however, cannot reach the same number of consumers or support the same number of content providers as efficient data-driven advertising.[146] It does not permit small and mid-size businesses as well as niche causes to target their messaging across the open Internet. Contextual advertising is inherently limited and would force the economy back towards a broadcast model of advertising that is inefficient, costly, and less useful for consumers and businesses alike.[147]

If only contextual methods of advertising remain available, charities that fund efforts to save animal species from extinction, for example, would not be able to effectively use ad space on properties unrelated to their cause to spread their messaging. Further, available spaces for advertising of general interest goods (such as toilet paper, razors, and dog food) would be severely limited because it is difficult—if not impossible—to determine (based on the context of a given website) that ads for such goods would be appropriate. Removing the ability to target messaging to pseudonymized consumers and dictating advertising content based solely on the content of a website with which the user currently interacts would remove value for website publishers, advertisers, and consumers. Studies also show that sole or primary reliance on contextual advertising is likely to advantage large publishers and well-established brands over their small business counterparts.[148]

In performing its cost-benefit analysis, the FTC must account for how data-driven messaging and advertising make the consumer experience better. Data-driven messaging allows pertinent information to reach individuals quickly and efficiently, and the efficacy of such

---

[143] *See* Jeremy B. Merrill & Drew Harwell, *Telling conservatives it's a shot to 'restore our freedoms': How online ads are promoting coronavirus vaccination*, WASH. POST (Aug. 24, 2021), https://www.washingtonpost.com/technology/2021/08/24/vaccine-ad-targeting-covid/.
[144] *Privacy ANPR* at 51283 (question 41).
[145] *Id*. (question 42).
[146] *See generally* JURA LIAUKONYTE, PERSONALIZED AND SOCIAL COMMERCE 12-23 (May 13, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3846888; JOHN DEIGHTON, THE SOCIOECONOMIC IMPACT OF INTERNET TRACKING, IAB (Feb. 2020), https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf.
[147] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 13-15 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.
[148] *Id*. at 11-12.

personalized communications cannot be replicated by turning to other existing methods of communicating with consumers. Data-driven advertising enables businesses of all sizes to reach consumers with relevant advertisements and messages. The myriad benefits that personalized, data-driven messaging provides to consumers should be an integral part of the Commission's consideration of the benefits that accrue from open access to and responsible use of data.

b. Data lowers barriers to entry for small and mid-size businesses and increases competition in the marketplace.

The open data ecosystem, free of unreasonable barriers to entry, is competitive and vibrant. Thousands of companies compete on a daily basis for consumer attention and patronage. Access to data enables smaller businesses to compete with the economy's largest players. Small businesses derive significant value from uses of data that would be lost by an overbroad regulation prohibiting their ability to reach target markets. In the Privacy ANPR, the Commission asks: "To what extent would any given new trade regulation rule on data security or commercial surveillance impede or enhance competition? Would any given rule entrench the potential dominance of one company or set of companies in ways that impede competition? If so, to what extent?"[149] Open access to data supports a lively, healthy economic ecosystem that permits small businesses to grow and reach new customers. The Commission's regulations should preserve the legitimate business communications and reasonable data practices that are foundational pillars of a competitive, diverse, and vibrant economic marketplace.

i. Data supports small businesses' ability to compete and grow.

Data-supported content helps consumers and publishers (especially Americans' favorite mom-and-pop shops, local bloggers, and other small businesses) connect with prospective customers. Data-driven methods allow for customization that creates a more enjoyable experience for consumers and uplifts small businesses to compete with companies that have already established themselves in the market.[150] Data-driven methods of prospecting are the basis of economic value for small and mid-sized publishers of the content consumers desire that do not have initial access to a large existing customer base. The FTC should consider how uses of data support the ability of small businesses to reach consumers and of content providers to provide free and low-cost ad-supported material to consumers. Access to a vibrant ecosystem of small businesses provides significant benefits by giving consumers options rather than forcing them into the hands of just a few established companies.[151]

Research demonstrates that preserving uses of data will bolster competition, increase the number of outlets available to consumers, and diversify the marketplace so small businesses can compete.[152] In a survey of 30,500 small businesses, 72% of U.S. businesses reported that data-

[149] *Privacy ANPR* at 51282 (question 27).
[150] DAA, Study: *Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), https://digitaladvertisingalliance.org/press-release/study-online-ad-value-spikes-when-data-used-boost-relevance.
[151] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 24-27 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.
[152] SBE Council, *Online Advertising Delivers BIG Benefits for Small Businesses* (Sept. 10, 2019), https://sbecouncil.org/2019/09/10/online-advertising-delivers-big-benefits-for-small-businesses/.

driven advertising is important to the success of their business.[153] 76% of U.S. small businesses surveyed stated that personalized ads in particular helped them find new customers.[154] For the small businesses that used data-driven advertising, sales growth was 16% greater than for small businesses that did not use data-driven practices.[155] Data-driven practices thus create efficiency for small enterprises, drive critical growth for those companies, and connect them to consumers who otherwise might never hear of products and services if they had to find those businesses on their own, without the assistance of targeted messaging.

ii. Third-party data is imperative for small businesses' success and growth.

Third-party data sets are a key driver of value for companies of all sizes. The ability to use data received from other entities in the marketplace allows first-party entities to improve their products and services, develop new useful offerings to benefit consumers, and more effectively reach consumers who may be interested in their products and services. One study found that in 2020, companies spent approximately $325.6 billion to promote their products and services, a figure that includes capital spent on third-party data sets to enrich targeted advertising campaigns.[156] In return, those companies realized approximately $2.8 trillion in sales, meaning that "every dollar of ad spending generated, on average, $8.6 in incremental sales."[157] Third-party data thus amplifies the efficiency and profitability of advertising campaigns, which fuels the economy and creates an environment where consumers have access to a variety of goods and services to meet their needs and desires.

With third-party data, first parties can move beyond the data they receive from direct consumer interactions to make use of other information to inform and optimize their marketing campaigns. In this way, third-party data is essential for small and mid-size companies with tight budgets to reach as many new potential customers as possible. One study of small businesses suggests that approximately 7 of 10 small firms in the U.S. report achieving a higher return on marketing spend through the use of personalized ads, which are (in part) powered by third-party data.[158] A majority of such small businesses also agreed that personalized ads, enabled by third-party data, "reduc[e] the costs of advertising."[159] Third-party data thus drives revenue and reduces costs for small enterprises, thereby empowering small and mid-sized businesses to compete actively with larger companies who may have more resources to allocate to broad marketing efforts. Third-party data can help companies better target marketing offers, unlock new revenue streams from recently unveiled products or services, improve risk mitigation and risk assessment efforts, and better foresee changes in demand for their products and services.

---

[153] *See* DELOITTE, DYNAMIC MARKETS: UNLOCKING SMALL BUSINESS INNOVATION AND GROWTH THROUGH THE RISE OF THE PERSONALIZED ECONOMY at 27 (May 2021), https://scontent-iad3-1.xx.fbcdn.net/v/t39.8562-6/10000000_4303078769743544_7237603050373993547_n.pdf?_nc_cat=109&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=jeXoHz0BKsMAX8IJfUR&tn=ek4tsdjsQsha6HLE&_nc_ht=scontent-iad3-1.xx&oh=00_AT8AudC54X2oXUppIyaLrYJiTxAmm23hvJvpcH19eUpQqA&oe=63452189.
[154] *Id.*
[155] *Id.* at 2.
[156] IHS MARKIT, THE ECONOMIC IMPACT OF ADVERTISING ON THE US ECONOMY 2018 – 2026 at 9 (Nov. 2021), https://www.ana.net/getfile/33850.
[157] *Id.*
[158] *See id.* at 27.
[159] *Id*.

In its proposed rulemaking, the FTC must weigh the costs of regulations that would restrict responsible uses of data (and consequently undermine competition and aid consolidation) against regulatory alternatives that would maintain access to data, including third-party data, on a more level playing field. Overly broad regulations or prohibitions on uses of data could have anticompetitive effects by making compliance extremely costly for small businesses while larger and more well-resourced businesses would be able to absorb the costs of compliance. By way of illustration, on average, companies exposed to the EU General Data Protection Regulation faced significant compliance costs and reduced ability to sell and market their offerings. Compliance costs accounted for more of such firms' overall losses than reduced sales. Small and medium-sized companies disproportionately bore this adverse effect.[160]

iii. Open access to data supports a healthy, competitive economy.

Regulations that do not strike the right balance between providing protections while permitting open access to data risk exacerbating market consolidation and intermediary control over data. The FTC should consider the wide breadth of uses and practices that data supports among highly diverse businesses and should ensure any regulations it promulgates do not entrench certain companies at the expense of others and negatively impact competition. Regulations should not enshrine in law some entities' ability to use "privacy" and their market power to force out competition in the marketplace and bolster their own lines of business.[161] The FTC is well-positioned to avoid perpetuating these anticompetitive behaviors. The Commission should further acknowledge the competitive benefits that open access to data provides and uphold reasonable data practices that support competition. Data rules should prevent platforms with the ability to control their competitors' access to data from exercising undue gatekeeping power when reasonable data collection and use is necessary to offer competitive services.

Intermediary companies' ability to control other businesses' access to consumers has already had significant effects on competition. For example, after Apple restricted access to its Identifier for Advertising ("IDFA"), the cost of acquiring new customers for businesses increased substantially to be, in some instances, 10 times more expensive than it was when the IDFA was widely available.[162] One small business reported that before use of the IDFA was restricted, it spent approximately $27 to gain a new customer via data-driven advertising.[163] After Apple's restrictions, that same small business reported spending $270 to acquire a single new customer, demonstrating the significant advertising cost hikes that small business suffered after Apple restricted the open flow of data.[164] According to the founder of the company, the cost increase was "a huge jump" that the company could not absorb.[165]

---

[160] *See generally* Carl Benedikt Frey & Giorgio Presidente, *The GDPR Effect: How Data Privacy Regulation Shaped Firm Performance Globally,* CEPR (Mar. 10, 2022), https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally.
[161] *Privacy ANPR* at 51283 (question 52).
[162] Patience Haggin & Suzanne Vranica, *Apple's Privacy Change Is Hitting Tech and ECommerce Companies. Here's Why*, WALL STREET J. (Oct. 22, 2021), https://www.wsj.com/articles/apples-privacy-change-is-hitting-tech-and-e-commerce-companies-11634901357.
[163] *Id.*
[164] *Id.*
[165] *Id.*

Other companies that control the ways businesses interact with consumers, such as browsers, also serve as intermediaries that stand to benefit from regulations that unreasonably restrict data flows. Such companies have begun taking steps to bolster their already well-established market positions by deprecating technologies that allow other firms to access data, while preserving their own ability to use consumer information for their own purposes. The impact of these systemic changes is that the behemoth intermediary companies that control so much of how commerce is effectuated online have undue power to restrict other companies from competing. This leads to increased market consolidation overall and monopolistic results, which are detrimental to the goal of sustaining a vibrant economy where small businesses can compete. The Commission should not create rules that require or incentivize companies to prevent the authorized collection of data through their services, leading to the creation of virtual "company towns" where data is entrenched with siloed services.[166] To do so would not only impede the ability of businesses to select with whom and how they do business but would also concentrate market power in a few firms and effectively eliminate new competitive entrants.

The FTC should consider carefully how any rules it issues to limit the availability of data would benefit large platforms and intermediaries while simultaneously harming all other businesses in the marketplace. The Commission should look to industry initiatives that are exploring ways to ensure access to data remains on an even playing field for all entities in the economy. The Partnership for Responsible Addressable Media ("PRAM"), for example, which is now housed within the DAA, has a mission of developing a framework for "addressable communications between consumers and businesses that safely leverage data."[167] PRAM's work involves creating interoperable standards for addressable media solutions that enable all businesses across browsers, devices, and platforms to equally access those solutions without unreasonable interference. Ensuring that all companies are subject to the same data rules that do not declare winners and losers in the marketplace (especially when that decision is based in large part on existing market power) will be key to maintaining a competitive, vibrant economy.

In order to promote competition, the FTC should consider how any proposed data regulations could have the unintended effect of removing opportunities for businesses to compete with larger, more well-entrenched players. A clear and well-rounded description of the benefits access to data provides to competition will help ensure any ensuing regulations further encourage access to data and responsible data use. The FTC should promote competition by permitting the responsible collection and use of data in the marketplace to support data-driven and other innovative business models that generate content, deliver consumer value, and grow the economy as a whole. This approach would capitalize on the benefits of data-driven practices while reducing costs to consumers and the economy.

---

[166] *Privacy ANPR* at 51283 (question 52); J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 29-30 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.

[167] *See* Partnership for Responsible Addressable Media, *Developing Addressability Solutions that Safeguard Privacy, Improve the Consumer Experience, and Protect Ad-Supported Digital Content and Services*, https://www.responsibleaddressablemedia.com/; *see also* Partnership for Responsible Addressable Media, *Policy Framework for Addressable Media Identifiers*, https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/AMI_Principles_Booklet.pdf.

VI. The FTC should evaluate the benefits of a risk-based approach to data security and the costs of overly restrictive or disharmonized security requirements that could result from Mag-Moss rulemaking.

If the FTC moves forward with its stated goal of promulgating data security rules through this Mag-Moss rulemaking, it should take a risk-based approach that accounts for companies' differing capacities to adopt various data security measures, such as the approach set forth in the Privacy for America *Framework* and the Commission's own Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule for financial institutions.[168] In the Privacy ANPR, the Commission asks: "Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?"[169] If the Commission addresses data security in a rulemaking, it should create a structure that incentivizes good-faith compliance with security standards rather than imposing inflexible mandates. Highly restrictive across-the-board mandates that do not consider the varying sophistication of entities and levels of risk to consumers presented by different kinds of data processing will fail to provide needed flexibility. Additionally, the FTC should not issue breach notification rules that unreasonably add to or conflict with existing notification requirements in all 50 states.

Instead of imposing one-size-fits all data security requirements that outline specific technical, organizational, or physical measures entities must take to bolster security, the FTC should provide a principles-based framework that allows companies to prioritize security in ways that make sense given the nature of the data they handle, their size and capabilities, and the risk of harm to consumers. Rulemaking should contemplate flexibility for companies in ways that allow them to tailor the form and function of their data security programs to particular risks faced and new developments in the marketplace. The FTC should also recognize accreditation programs that certify companies' data security programs to help ease enforcement burdens on the Commission and incentivize compliance in the marketplace. Compliance with an FTC-accredited data security program should be considered a safe harbor for enforcement actions that claim the company failed to meet required standards for data security based on a novel or unexpected breach of security (potentially by a foreign state actor).

The FTC also should not consider breach notification rules in this rulemaking effort. The information supporting the FTC's examination of "data security" in the ANPR focuses primarily on physical, technical, and administrative procedures to protect data.[170] However, the ANPR's proposed definition of "data security" is broadly constructed to mean "breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices."[171] The United States already has 50-plus state laws setting forth data breach notification requirements. These existing state laws serve the purpose of informing consumers of a breach and providing mediating services, like credit monitoring, in the event of breaches

[168] 16 C.F.R. § 314.1 *et seq*.; *Privacy for America*, Part I, Section 3(N), https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/.
[169] *Privacy ANPR* at 51281 (question 11).
[170] *Id.* at 51282-83.
[171] *Id*. at 51277.

involving certain kinds of information. Over nearly two decades, Congress has considered but has never passed a federal breach notification law, opting instead to leverage the work that already has occurred in the states to define standards for breach notification. The FTC should not use its present rulemaking effort as an opportunity to reopen the subject of breach notification requirements.

Any data security rules that are the subject of the FTC's rulemaking should provide guiding principles rather than hard and fast requirements to implement particular security measures. Rules with that flexibility would be a similar balance that the Commission struck in the GLBA Safeguards Rule, a set of requirements for financial institutions that take into account the varying size and complexities of that sector of the economy.[172] Such an approach would allow both large and small businesses to appropriately secure information and balance their security efforts against the risk of potential harm to individuals. This type of risk-based regulation is especially important given the potential scope of the FTC's actions; applying the same security requirements to mom-and-pop corner stores and Fortune 50 companies would not be appropriate, reasonable, or responsible. The Commission should focus its efforts on setting forth a risk-based framework to evaluate reasonable security procedures that is tailored to the nature of the security risk presented by a particular context and business model. In considering data security rules, the FTC should keep in mind existing federal and state requirements to ensure its regulations do not overlap or conflict with existing obligations. As the Commission looks to improve data security across the economy, it should construct rules that harmonize with existing requirements and support companies' good faith compliance efforts.

* * *

Thank you for the opportunity to provide comments on the Privacy ANPR. While we disagree that the Commission's approach is the best way to address data privacy on a nationwide basis, we appreciate the FTC's engagement in the space. We hope that, at a minimum, the responses to the Privacy ANPR can serve as additional background for Congress to continue its work on preemptive, comprehensive privacy legislation. Please contact Stu Ingis, Counsel to Privacy for America, at singis@venable.com with any questions regarding this submission.[173]

Sincerely,

Privacy for America

[172] 16 C.F.R. § 314.1 *et seq*.

[173] A selection of the research papers and studies cited in this comment are attached in Appendix A.