BEFORE THE FEDERAL TRADE COMMISSION

Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex B)
Washington, D.C. 20580

COMMENTS

of

NETWORK ADVERTISING INITIATIVE

on the

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

"Commercial Surveillance ANPR, R111004"

Leigh Freund
President & CEO
Network Advertising Initiative

Introduction and Executive Summary

Thank you for the opportunity to comment on the Advanced Notice of Proposed Rulemaking ("ANPR") for a Trade Regulation on Commercial Surveillance and Data Security.

The Network Advertising Initiative ("NAI") strongly supports the establishment of greater privacy protections for consumers that extend beyond what U.S. federal laws and regulations currently require, and firmly believes that the path to such protections lies in the passage of comprehensive federal privacy legislation. While the NAI agrees with the stated goal of providing clear rules of the road that foster a "greater sense of predictability for companies and consumers and minimize the uncertainty that case-by-case enforcement may engender,"[1] we do not believe that promulgating regulations in the absence of federal privacy legislation is the correct approach to providing such clarity.

We are proud that the NAI, through its industry-leading self-regulation, has been able to impose strong privacy protections for consumers over more than two decades. We believe, however, that the time has come for a comprehensive national privacy framework to provide clear rules for all companies, not just those volunteering to submit to such standards, as well as additional privacy enhancements for consumers. The NAI is skeptical that a rulemaking procedure is able to achieve the broad and uniform framework that is needed by consumers and businesses alike.

Therefore, the NAI continues to urge congressional lawmakers to enact a national privacy law that provides a clear, consistent set of requirements for all businesses operating in the United States, and to replace the disparate patchwork of state consumer privacy laws that is developing across the country. Such a framework should ban certain uses of data and allow for innovative uses of data for advertising and the social good.

The NAI is proud to have worked closely with the Federal Trade Commission ("FTC" or "Commission") for over two decades, as it developed into a leading regulator of consumer data privacy and security, not just in the United States, but around the world. Since our inception, the NAI has engaged with commissioners and staff as they have developed new policies, and has evolved our self-regulatory efforts to keep pace with these policies, as well as technological and process developments across the digital marketplace.

The NAI believes Congress is best positioned to develop nationwide privacy standards. While we recognize that regulators and policymakers at the FTC have a statutory responsibility to protect consumers from unfair and deceptive acts or practices, we are concerned that the overly expansive scope of the ANPR, particularly the broad brush with which it paints virtually all business practices that collect and process consumer data as "commercial surveillance," unjustly characterizes many beneficial business practices that do not harm consumers. In addition, it raises questions about whether the Commission should engage in a rulemaking to establish broad prohibitions that exceed the FTC's statutory authority. While the ANPR raises a wide range of questions about the potential courses the Commission may take with a Section 18 rulemaking, it appears to suggest that the

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,276 (proposed Aug. 22, 2022).

Commission has already determined that a substantial majority of current business practices should be prohibited through a rulemaking.[2]

The NAI is also troubled by assertions in the ANPR and by other stakeholders that third-party companies present heightened risks to consumers because of their limited visibility, in the mistaken belief that their processing of consumer data is unexpected and should be prohibited.[3] The NAI strongly disagrees with this perspective. The NAI's self-regulatory standards were created over twenty years ago by third-party companies in the digital advertising space to demonstrate a public willingness to offer consumer choice and protect consumer data precisely because of their limited visibility. At the same time, many first-party companies have been found on myriad occasions to be poor data stewards and directly responsible for informational injuries to their consumers. We believe that there should be clear, consistent rules that apply equally to all parties collecting and using consumer data, regardless of where they sit in the ecosystem, and that federal legislation with data use limitations can best provide such consistency.

In the absence of a new law creating a national privacy framework to apply uniformly across the entire industry, the NAI believes there are steps the Commission can take to bolster broadly-held consumer data privacy and security goals. These comments propose the following constructive alternatives to the Commission engaging in an overly-expansive rulemaking process.

- Empower and promote self-regulatory organizations and standards that can amplify the objectives of the Commission. Self-regulation can provide additional value where the Commission's limited resources do not provide for engaging directly with a wide range of companies, and it can actively encourage compliance with legal requirements and best practices.
- Maximize competition across the digital advertising ecosystem by focusing more precisely on the harmful uses of data, and the implementation of data stewardship requirements across all of industry, first-party and third-party alike, rather than seeking to limit data sharing with service providers and third parties for advertising and marketing.
- Bolster the role of transparency and consumer control through clear guidance, rather than denouncing this framework as ineffective and obsolete, while seeking to establish broad data collection and use restrictions.

[2] *Id.* at 51,282 (Section I: ". . . the Commission is beginning to consider the potential need for rules and requirements regarding commercial surveillance and lax data security practices"; Section III(b): "A trade regulation rule could provide clarity and predictability about the statute's application to existing and emergent commercial surveillance and data security practices that, given institutional constraints, may be hard to equal or keep up with, case-by-case.")

[3] *See generally* Fed. Trade Comm'n, Commercial Surveillance and Data Security Public Forum (Sept. 8, 2022), https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.

I. The NAI Is the Leading Self-Regulatory Association for the Advertising Technology Industry

a. About the NAI

The NAI is the leading self-regulatory organization dedicated to responsible data collection and use by advertising technology companies engaged in Tailored Advertising and Ad Delivery and Reporting (ADR).[4] For over 20 years, the NAI has promoted a robust digital advertising industry by maintaining and enforcing the highest voluntary standards for the responsible collection and use of consumer data for digital advertising. Our member companies range from large multinational corporations to small startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation.

All NAI members are required to adhere to the NAI's FIPPs-based,[5] privacy-protective Code of Conduct ("NAI Code" or "Code"), which continues to evolve and underwent a major revision in 2020 to keep pace with changing business practices and consumer expectations of privacy.[6] In some cases, the NAI Code creates requirements that extend further than existing legal and other self-regulatory requirements. For example, since its founding in 2000, the NAI has restricted responsible actors in the digital advertising ecosystem from merging, or combining, cross-site or cross-app information with directly identifying information. Perhaps one of the unfortunate consequences of recent legislation, which defines nearly all data points as Personal Information, without any apparent restrictions on commingling and otherwise combining that data, is the dilution of the relative sensitivity of some of these diverse data points, and the potential for the normalization of the merger of cross-site browsing information with directly identified consumers. The NAI was founded in part to help prevent the linking of browsing information, and later information from other media, with directly identified individuals. Further, NAI members are restricted from making inferences based on web browsing, app use, or digital content viewership that can point to user interest in treatments or medications for a variety of sensitive conditions, including mental health treatments, sexually-transmitted infections, cancer, and children's health conditions that cannot be treated with over-the-counter medication without the opt-in consent of the user. Many other examples are detailed below.

---

[4] Tailored Advertising is defined by the NAI Code as the "use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device." Ad Delivery and Reporting is "separate and distinct from Tailored Advertising, and it refers to the collection or use of data about a browser or device for the purpose of delivering ads or providing advertising-related services, including, but not limited to: providing a specific advertisement based on a particular type of browser, device, time of day, or real-time precise location; statistical reporting, traffic analysis, analytics, optimization of ad placement; ad performance, reach, and frequency metrics (including frequency capping); sequencing of advertising creatives; billing; and logging the number and type of ads served on a particular day to a particular website, application or device. ADR does not include data collection and use for security and fraud prevention." *See* Network Advertising Initiative, 2020 NAI Code of Conduct § I.A, I.Q (2020), https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

[5] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[6] *See* NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter "NAI Code"], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

Member compliance with the NAI Code is promoted by a strong accountability program. NAI compliance staff subject each member to a comprehensive annual review of their products, practices, partner contracts, privacy policies, and consumer-choice mechanisms for adherence to the NAI Code, advising members on an ongoing basis about how best to comply with the Code and guidance. The NAI relies on the insights from these annual compliance reviews to identify and close any potential gaps in the Code, and to address new technologies and products developed by member companies. As the pace of innovation in the advertising technology industry continues to accelerate, the NAI will consistently revise the Code in order to address novel products, technologies, and applications by member companies, based largely on insights obtained through the valuable compliance review process.

The NAI team also conducts technical monitoring and review of company opt outs and privacy tools. The NAI's enforcement efforts focus on ensuring members' rapid curing of deficiencies in good faith, but enforcement of the NAI Code can also include penalties and sanctions for material violations. The NAI reserves the discretion to refer violations to the FTC, particularly if companies refuse to implement required remedies or attempt to mislead NAI staff. Such referrals have historically not been necessary, as members value the NAI's feedback and the reputational benefit of membership. Consequently, members overwhelmingly provide swift resolution of relevant problems.

b. NAI Guidance and Best Practices Align with the FTC's Goals

In addition to our industry-leading Code of Conduct, the NAI continues to assess gaps in the U.S. regulatory framework. Staff monitor state and federal legal and regulatory developments, and the Code evolves to reflect–and in some cases exceed—those requirements. Over the last few years, the NAI has published guidance in step with the Commission's positions, including guidance for the responsible use of precise location information ("PLI") for non-marketing purposes,[7] best practices for user choice and transparency to avoid "dark patterns,"[8] and draft guidelines for the use of deterministic shared addressability identifiers.[9] Most recently, the NAI collaborated with member companies that specialize in the collection of location-based information to craft a set of Precise Location Information Provider Voluntary Enhanced Standards ("Enhanced Standards") for processing and sharing of PLI that exceed legal requirements.[10] While currently voluntary for NAI members, it is our hope that demands for increased privacy protections in this area will spur NAI members and non-members alike to adopt these standards broadly.

---

[7] *See* NETWORK ADVERTISING INITIATIVE, Best Practices: Using Information Collected for Tailored Advertising or Ad Delivery and Reporting for Non-Marketing Purposes (2020), https://thenai.org/wp-content/uploads/2021/07/nai_nonmarketing-bestpractices-0620_final-1.pdf.

[8] *See* NETWORK ADVERTISING INITIATIVE, Best Practices for User Choice and Transparency (2022), https://thenai.org/wp-content/uploads/2022/05/NAI-Dark-Patterns-Final-5.12.22.pdf; *See also* Ryan Smith, *Takeaways for Digital Advertising Businesses from the FTC Staff Report on Dark Patterns*, Network Advertising Initiative (Oct. 20, 2022), https://thenai.org/takeaways-for-digital-advertising-businesses-from-the-ftc-staff-report-on-dark-patterns/.

[9] *See* NETWORK ADVERTISING INITIATIVE, Draft NAI Guidelines for Deterministic Shared Addressability Identifiers (2022), http://thenai.org/wp-content/uploads/2022/03/Draft-NAI-Deterministic-Addressability-Guidelines.pdf.

[10] *See* NETWORK ADVERTISING INITIATIVE, NAI Precise Location Information Solution Provider Voluntary Enhanced Standards (2022), https://thenai.org/wp-content/uploads/2022/06/Precise-Location-Information-Solution-Provider-Voluntary-Enhanced-Standards.pdf.

The breadth of the NAI Code and the rigor of the NAI compliance program positions NAI members well to respond and adapt to the FTC's policy and enforcement initiatives. For example, in September 2021 the FTC announced a policy statement that clarified the scope of its Health Breach Notification Rule (16 C.F.R. § 318.2).[11] The NAI amplified this policy statement to members,[12] noting that it aligned closely with requirements adopted in the 2020 NAI Code regarding the collection and use of sensitive data, as well as our guidance more broadly pertaining to sensitive health data.[13]

II. The FTC Should Leverage Strong Self-Regulation to Increase Participation and Adherence by Businesses in Order to Achieve its Goals

The ANPR contemplates a role for self-regulation in this rulemaking, and inquires as to what extent the self-regulatory model could be effective in mitigating harm.[14] Self-regulation, while not obviating the need for strong legal regulations and enforcement, can be further empowered as a framework that complements and bolsters the Commission's goals in two key ways.

First, self-regulation serves to extend and amplify the Commission's policies and enforcement goals, helping to compensate for the Agency's limited resources across a vast commercial marketplace. For example, a model such as the NAI's continually evolving guidance and annual review of member companies provides an opportunity to not only scrutinize company compliance with our own privacy protective requirements, but also to highlight the latest updates from federal and state regulators, and help companies identify potential regulatory infractions before they occur. This model can provide a valuable service for both responsible companies and the Commission, but depends on cooperation between the Commission and other regulators with self-regulatory organizations and the establishment of clear enforcement guidelines about evolving regulations.

Second, self-regulation offers a bridge between industry and policymakers that enables the creation of voluntary standards that address avoidable legislative gaps and shortcomings. For example, NAI's annual compliance reviews require staff to interface with lawyers, product developers, and even CEOs of member companies on a regular basis. This provides unparalleled insight into new business practices and technologies deployed by our members, and allows us to react in a timely manner and implement needed safeguards that are tailored to the digital advertising industry. For instance, the NAI's recently released Enhanced Standards were developed based on conversations with member companies, stakeholders, and regulators, who identified the need to address the use

[11] Press Release, Fed. Trade Comm'n, FTC Warns Health Apps and Connected Device Companies to Comply with Health Breach Notification Rule (Sept. 15, 2021) (https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health-breach-notification-rule).

[12] Network Advertising Initiative, NAI Regulatory Summary and Analysis: Statement of the Federal Trade Commission on Breached by Health Apps and Other Connected Devices (Feb. 2022), https://thenai.org/nai-regulatory-summary-and-analysis-statement-of-the-federal-trade-commission-on-breaches-by-health-apps-and-other-connected-devices/.

[13] *See* NAI Code.

[14] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51,282, (proposed Aug. 22, 2022) (Question 30, "Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extralegal measures, including self-regulation, sufficient? To what extent, if at all, are self-regulatory principles effective?).

of contextual information with sensitive locations, such as abortion clinics and places of worship.[15] Notably, this work *predated* the *Dobbs v. Jackson Women's Health Organization* Supreme Court decision, which spurred lawmakers and regulators, including the Commission, to embrace similar standards. What is more, as noted above, our relationship with members and knowledge of the industry prompted an update to the 2020 NAI Code that expanded requirements around sensitive data that mirrored the Commission's 2021 policy statement regarding the health breach notification rule for non-HIPAA entities.

The NAI strongly supports a federal consumer privacy law that applies consistently across the entire industry, and establishes a formal role for self-regulatory organizations to work cooperatively with federal and state regulators, with strong oversight and accountability mechanisms. In the absence of such a law, the FTC can achieve the goals of enhancing consumer privacy and data protection by promoting greater participation with self-regulatory organizations. For companies, there is a business case for joining an organization such as the NAI. Advertisers and digital publishers have long demonstrated a preference for working with NAI members, who are identified across the marketplace as prioritizing heightened consumer data privacy standards. Greater participation in self-regulatory organizations also provides a substantial benefit to the FTC, as it provides another means for companies to be scrutinized and create a distance from bad actors, and the Commission gains enhanced enforcement opportunities against those higher commitments these companies make.

Again, while a national privacy law is the ideal path for empowering self-regulatory organizations to amplify and help enforce legal requirements, the Commission has the ability to empower leading self-regulatory organizations through targeted industry initiatives and to encourage greater participation through renewed outreach to industry. The NAI was created as a result of support from the Commission and other U.S. policymakers who recognized the added value we could provide, and we believe that the value is increased today, not diminished. If the Commission should decide to engage in a rulemaking, it should use that as an opportunity to enable any new regulations to be elevated through self-regulatory organizations working in tandem.

I. Data Driven Advertising Powers the Rich Digital Media Industry, Benefiting Consumers, Publishers and Small Businesses

The digital advertising industry helps maintain the free and open internet, and is composed of multiple sectors – primarily advertisers, advertising agencies, publishers (including a wide range of digital content and service providers), and advertising technology companies. Each sector includes businesses ranging dramatically in size, from startups to large, multinational companies. Digital advertising includes a diverse and evolving set of products and services that together help promote the thriving digital media ecosystem, including tailored advertising, contextual advertising, and search advertising, among others. This range of products and services creates a competitive marketplace that serves well established and new businesses alike as they engage with existing customers and try to reach new audiences across the digital media landscape.

[15] See Network Advertising Initiative, NAI Precise Location Information Solution Provider Voluntary Enhanced Standards (2022), https://thenai.org/wp-content/uploads/2022/06/Precise-Location-Information-Solution-Provider-Voluntary-Enhanced-Standards.pdf.

a. Consumers

Tailored advertisements, as opposed to contextual, or direct-buy ads, improve the consumer's experience and access to quality digital products and services. Not only is tailored advertising more relevant, more interesting, and more likely to produce engagement, it also funds publishers and digital service providers. Advocates of contextual advertising have tried to claim that contextual advertising can generate the same amount of revenue without any of the downsides; however this claim is not backed by solid evidence.[16] If that were the case, publishers and digital media providers would be voluntarily using them, but instead rely most heavily on tailored advertising because this is more effective and thus generates more revenue.[17] The digital media industry has experienced robust growth over the last two decades, providing transformative benefits such as access to rich, quality content to consumers for free, or little cost.

The FTC Bureau of Economics recognized this conclusion in a 2020 paper, noting that data suggests tailored ads create consumer surplus, as search costs decrease for both the consumer and the seller.[18] The report concludes that consumers have access to valuable digital goods and services as a result of data driven tailored advertising revenue. In the absence of such advertising, consumers would likely pay in dollars, which has been predicted to "disproportionally affect more wealth-constrained users, who may end up losing access to these free services."[19] The report also recognizes the potential detrimental effects of tailored advertising and concludes that "policy decisions in this arena must account for all these various aspects of economic analysis."[20] Indeed, the NAI agrees with the conclusion of the report that when public policies ensure that consumers are given the accurate and clear information they need to make informed choices, consumers continually choose the free and low cost digital media that tailored advertising supports. Findings and conclusions such as these, recognizing the role and value of tailored advertising, have been consistently recognized by the Commission for more than two decades in publications, prepared statements, appeal decisions, and reports to Congress.[21]

---

[16] Daniel Castro, *No, Contextual Advertising Is Not a Substitute for Targeted Advertising*, Center For Data Innovation (Nov. 29, 2021), https://datainnovation.org/2021/11/no-contextual-advertising-is-not-a-substitute-for-targeted-advertising/.

[17] *Id.*

[18] Fed. Trade Comm'n, A Brief Primer on the Economics of Targeted Advertising from the Bureau of Economics 2-3 (Jan. 2020), https://www.ftc.gov/reports/brief-primer-economics-targeted-advertising.

[19] *Id.*

[20] *Id.*

[21] *See In re 1-800 Contacts, Inc. , 2018 FTC LEXIS 184, *58 (Fed. Trade Comm'n Nov. 7, 2018)* (the opinion of the Commission is that "[r]estrictions on advertising interfere with that flow of information and raise the cost to consumers of finding the most suitable offering of a product or service… [and] "as a result of the reduced information flow, some consumers will pay higher prices for the particular good or service while others stop their search before they find a price that induces them to buy, which reduces the quantity sold."), *see also, e.g.,* Fed. Trade Comm'n, Cross-Device Tracking: an FTC Staff Report (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf ("cross-device tracking technology may enhance competition in the advertising arena"); Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf ("Big data analytics can provide numerous opportunities for improvements in society"); Prepared Statement of the FTC on Emerging Threats in the Online Advertising Industry Before the Senate Committee on Homeland Security and Governmental Affairs (May 15, 2014),

Consumers place a high value on their online content and services. A 2018 study found that the median consumer values e-Commerce at $842 per year, social media at $322, streaming music at $168 per year, and Instant Messaging at $155 per year.[22] NAI research on the topic also revealed that consumers are disinclined to pay more for their online content than they already do. A consumer survey in 2019 revealed that nearly 60 percent of respondents prefer their online content to be paid for by advertising, and nearly 90 percent said they are unwilling to pay a significant amount of money to continue receiving apps and online content that they currently receive for free—a strong affirmation that an ad-supported content model is ideal for consumers.[23]

Additionally, research also suggests consumers prefer ads tailored to their personal preferences. A 2016 study found 71 percent of respondents preferred online advertisements that were influenced

---

https://www.ftc.gov/system/files/documents/public_statements/309891/140515emergingthreatsonline.pdf ("Online advertising offers many benefits to consumers. . . It also can be used to tailor offers for products and services most relevant to consumers' interests."); Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("the collection and use of consumer data has led to significant benefits in the form of new products and services. . . The Commission recognizes the need for flexibility to permit innovative new uses of data that benefit consumers"); Prepared Statement of the FTC on The State of Online Consumer Privacy Before the Senate Committee on Commerce, Science, and Transportation (Mar. 16, 2011), https://www.commerce.senate.gov/services/files/C7C4C0F5-B665-488D-A372-4F09DD17E32C ("the roundtable commenters and participants urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information"); Prepared Statement of the FTC on Do Not Track Before the House of Representatives Committee on Energy and Commerce (Dec. 2, 2010), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-do-not-track/101202donottrack.pdf ("In considering a uniform choice mechanism for online behavioral advertising, the Commission recognizes the benefits of such advertising, which helps support some of the online content and services available to consumers and allows personalized advertising that many consumers value"); Where's the Remote? Maintaining Consumer Control in the Age of Behavioral Advertising, Remarks of FTC Chairman Jon Leibowitz at the National Cable & Telecommunications Association (May 12, 2010), https://www.ftc.gov/sites/default/files/documents/public_statements/wheres-remote-maintaining-consumer-control-age-behavioral-advertising/100512nctaspeech.pdf ("The FTC does not want to shut down responsible business practices or stifle innovative and efficient uses of the online marketplace – and we don't plan to do so. We want only, as behavioral advertising develops and spreads, to protect those two pillars of the growing, changing, thriving cyber-world: consumer choice and consumer control."); Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf (FTC reports on online profiling's benefits to consumers); Prepared Statement of the FTC on Behavioral Advertising Before the Senate Committee on Commerce, Science, and Transportation (Jul. 9, 2008), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-behavioral-advertising/p085400behavioralad.pdf ("[B]ehavioral advertising may provide benefits to consumers in the form of advertising that is more relevant to their interests. Consumer research has shown that many online consumers value more personalized ads."); Online Profiling: A Report to Congress (June 2000), https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf ("Network advertisers' use of cookies and other technologies to create targeted marketing programs also benefits both consumers and businesses.")

[22] *See* Erik Brynjolfsson et al., *Using Massive Online Choice Experiments To Measure Changes In Well-Being*, Nat'l Bureau of Econ. (Apr. 2018), https://www.nber.org/system/files/working_papers/w24514/w24514.pdf.

[23] *See* Network Advertising Initiative, Consumer Survey on Privacy and Digital Advertising (Oct. 22, 2019), https://thenai.org/wp-content/uploads/2021/07/final_nai_consumer_survey_paper_22oct2019.pdf.

by their interests and habits as compared to purely contextual ads.[24] Another survey from 2019 conducted found 90 percent of consumers consider advertising content from companies not personally relevant to their interests "annoying," with 53 percent saying ads for an irrelevant product are the "most annoying."[25] Support is particularly strong among Millennials, who consider personalization "critical" to earning and keeping their business.[26] In fact, Millennials and Generation Z are overwhelmingly comfortable with companies using relevant information about them in exchange for personalized advertisements and in fact, even expect it.[27] Ultimately, consumers enjoy the benefits personalized ads provide, and it would degrade their online experience if the digital media ecosystem is forced to adapt without tailored advertising.

b. Small Businesses and Direct to Consumer Brands

The ANPR inquires about the cost differential between tailored and contextual advertising.[28] For many companies, tailored advertising is the most cost-effective method to reach existing customers and to generate new ones, as it helps companies of all sizes reach customers that are most likely to be interested in their products and to interact with the ads. Tailored advertising is particularly beneficial for small business advertisers—those without a dedicated ad-sales team– working with limited marketing and ad budgets, in competition with dominant, vertically integrated sellers. Tailored advertising facilitates competition by optimizing the resources of small businesses to scale, leveling the playing field and allowing them to more effectively compete with the large online platforms, or "walled-gardens," that enjoy a substantial advantage in generating data-driven advertising revenue.[29] This approach contrasts starkly with the contextual advertising model, where the same business would spend a higher percentage of its budget advertising to a broader set of consumers, many of whom are less likely to become customers.[30]

Tailored advertising also allows small and large businesses alike to maximize the efficiency of their ad-spend by identifying marketing trends and using their marketing budgets to directly reach audience segments that are seeking their products. In fact, data reveals small businesses that utilize

---

[24] *See* Holly Pauzer, *71% of Consumers Prefer Personalized Ads*, ADLUCENT (2016), https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/.

[25] *See* Tom Zawacki, *Why Consumers Prefer Personalization*, infogroup (2019), https://multichannelmerchant.com/blog/why-consumers-prefer-personalization/.

[26] *Id.*

[27] *See State of the Connected Customer*, Salesforce Research (Apr. 2019), https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/briefs/customer-trust-trends-salesforce-research.pdf

[28] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51,283 (Question 42, "How cost-effective is contextual advertising as compared to targeted advertising?").

[29] *FTC v. Polygram Holdings, Inc.*, 416 F.3d 29 (D.C. Cir. 2005) ("the Court repeatedly has recognized that advertising facilitates competition"); *FTC v. California Dental Association*, 526 U.S. 756 (1999) ("We believe in the basic premise, as does the Supreme Court, that by providing information advertising serves predominantly to foster and sustain competition, facilitating consumers' efforts to identify the product or provider of their choice and lowering entry barriers for new competitors.").

[30] Australian Competition & Consumer Comm'n, Digital Platforms Inquiry: Final Report 132 (2019), https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (finding that digital advertising benefits small businesses by providing them with "an ability to specifically target relevant audiences and by providing advertisers with an additional channel to reach consumers, often at a lower cost than traditional forms of advertising.").

tailored advertising are sixteen times more likely to report sales growth as opposed to competitors who do not.[31] By leveraging data for measurement and attribution, advertisers can easily determine how many consumers are engaging with their ads, as well as the sites, apps and content that provide for the highest level of engagement.

A growing and increasingly important segment of the e-commerce marketplace are direct to consumer ("D2C" or "DTC") brands that sell products directly to customers online while bypassing third-party retailers and wholesalers—often resulting in lower costs and pricing for consumers.[32] This industry, while still relatively small in terms of the overall U.S. economy, is vital and rapidly growing, often outpacing traditional suppliers of goods and services.[33] A recent forecast predicted D2C e-commerce sales will reach $151.2 billion this year, an increase of over 15 percent compared to 2021.[34] The study revealed that, "while this will only account for 2.5 percent of total retail sales, these brands have challenged and successfully disrupted the retail industry by diversifying consumer experience."[35] In fact, many large traditional U.S. businesses are embracing this model for some of their own niche products and relying more heavily on direct sales. This business model is revolutionary for its ability to provide high-quality goods and services to consumers, and serving niche segments of consumers interested in fashion, fitness, gourmet food, etc.

D2C companies, and other small, newly formed businesses serving specific customer bases are particularly dependent on tailored advertising due to the nature of their business models and dependence on reaching niche audiences via the internet. Using only contextual advertising, these companies would suffer, unable to reach their target consumer base efficiently. Over 90 businesses such as these signed a letter to the Commission from the organization Internet for Growth in November 2022, arguing that the elimination of third party data-driven advertising "could be devastating for many small businesses – and the millions of Americans they employ …," and that "[p]olicy changes of [this scale] would fundamentally remake the ad-supported digital economy, which accounts for 12% of GDP.[36] It is without a doubt that small businesses see the value in this form of advertising as they vote with their feet. A 2022 survey of small businesses found that 70 percent invest in social media advertising, with 54 percent planning to increase their current spend citing a wide range of benefits.[37] Empirical research from 2022 supports this fear among small businesses about the loss of data-driven advertising; such businesses would see a 37 percent

---

[31] Deloitte Dynamic Markets, Small Business Through the Rise of the Personalized Economy (2021).

[32] V. Kasturi Rangan, Daniel Corsten, Matt Higgins, & Leonard A. Schlesinger, *How Direct-to-Consumer Brands Can Continue to Grow*, Harvard Bus. Rev. (Nov. 2021), https://hbr.org/2021/11/how-direct-to-consumer-brands-can-continue-to-grow.

[33] Direct-to-consumer (D2C) e-commerce sales in the United States from 2019 to 2024, Satista (2022), https://www.statista.com/statistics/1109833/usa-d2c-ecommerce-sales/.

[34] *See generally* INSIDER INTELLIGENCE, INDUSTRY INSIGHTS: SPOTLIGHT ON D2C (Dec. 2021).

[35] *Id*.

[36] Letter from Internet for Growth to the Federal Trade Commission (Nov. 10, 2022) https://internetforgrowth.com/wp-content/uploads/2022/11/I4G-sign-on-letter_FINAL_11.10.22.pdf, citing John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, Interactive Advertising Bureau, 5, (Oct. 18, 2021).

[37] Anna Peck, *2022 Small Business Advertising Report*, Visual Objects (Mar. 14, 2022), https://visualobjects.com/advertising/blog/small-business-advertising-2022.

increase in the costs of acquiring new customers without offsite data.[38] Compared to larger scale advertisers, smaller advertisers rely more heavily on effective ads, and would be disproportionately hurt by the loss of offsite data at every point in measurable ad distribution.[39] As such, tailored advertising is essential for these companies to compete with large mainstream sellers with larger, more robust advertising budgets.[40] Without it, D2C and other small businesses would struggle to compete.

c. Publishers and Digital Content Providers

For publishers, providers of digital content and services, and other sites that offer ad space for purchase, tailored advertising is also extremely important. By using data to provide ad placements that are more likely to reach a business' target audiences, publishers are able to sell these placements for a premium. This often means publishers can show fewer ads, and decrease the need for paywalls to fund their content, while also improving user experience and reducing irrelevant ads.

Tailored advertising particularly benefits smaller publishers and app providers who lack the resources to negotiate directly with larger advertisers. These small businesses can rely on ad-tech companies to make their ad inventory available to a broad array of advertisers interested in displaying ads based on consumer interests, not just the content the ads will appear alongside. This is crucial for sites that specialize in a specific, or narrow set of topics, allowing them to serve their customers with a wide range of relevant ads for products and services that do not relate directly to their niche content but rather, to the interests of their visitors.

Research has consistently reflected the increased value of tailored advertising over traditional digital ads for publishers and digital content providers. Data suggests that the inability to target consumers resulted in a loss of $8.58 in ad-spend per user, a decrease in value over 50 percent.[41] Further, studies on the value of data for ad pricing show that targeting ads generally increases ad prices by a factor of two to three.[42] These economic implications are even more pronounced among

---

[38] Nils Wernerfelt et al., *Estimating the Value of Offsite Data to Advertisers on Meta* (Becker Friedman Inst. for Econ. at the Univ. of Chi., Working Paper No. 2022-114, 2022), https://bfi.uchicago.edu/wp-content/uploads/2022/08/BFI_WP_2022-114.pdf.

[39] *Id.* at 3, 26.

[40] *See* Competition and Mkt. Auth., *Online Platforms and Digital Advertising: Market Study Final Report*, 45 (2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

[41] *See* Johnson, Shriver, Du, *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?* (Last revised: Jan. 9, 2020).

[42] These studies predominantly relied on third-party cookie data as a measurement, given that cookies have historically been the primary method for enabling tailored advertising, *see, e.g.,* Sarah Sluis, *Marketing Professor Garrett Johnson Wants You To Know that Cookies Increase Ad Revenue*, ADEXCHANGER (Sept. 3, 2019), https://www.adexchanger.com/online-advertising/marketing-professor-garrett-johnson-wants-you-to-know-that-cookies-increase-ad-revenue/.;
see Johnson, Shriver, Du, *supra* note 17 (finding that absent cookies, ad revenue decreased by 52 percent based on a study of users opting-out using the AdChoices program).
see Ravichandran & Korula, *Effect of disabling third-party cookies on publisher revenue*, Google (2019), https://www.blog.google/products/ads/next-steps-transparency-choice-control/ (finding that absent cookies, ad revenue decreased by 52 percent based on an analysis of Google's top 500 publishers);

news publishers, as one study concluded that news publishers showing ads to consumers where no data was present generated 62 percent less revenue.[43] Of particular note, and in response to the ANPR questions 40 and 42 that inquire about the use of contextual advertising as an alternative, research from 2011 and 2019 reveals that news and general content websites are disproportionately affected negatively, and therefore less likely to deploy contextual advertising while generating similar revenue.[44] These findings are consistent with 2014 research by Eisenach and Beales, concluding, "cookies appear to be particularly valuable to companies that lack alternate sources of information about the user," such as smaller publishers.[45]

A single 2019 study is often referenced by opponents of data-driven advertising, suggesting that ad value decreased by only 4 percent in the absence of third-party cookies.[46] However, this study is the only known outlier among similar research, and was not subject to the same peer review and publishing process as the more prominent studies. As such, these conclusions should be approached with caution. The methodology lacks clarity, and the conclusions from this study have been substantially refuted as lacking a sound methodology, including in comments to the Commission in response to this ANPR.[47]

While much of the research to date is based on data pertaining to third-party cookies, the conclusion that advertisers will pay higher prices for tailored advertising extends more broadly. Therefore, the NAI and many of our members and partners in the industry are actively exploring a range of privacy enhancing technologies as alternatives to third-party cookies and other traditional pseudonymous device-level identifiers to capture the value of tailored advertising while minimizing privacy risks. A broad shift away from tailored advertising would deprive publishers, particularly small and medium-sized news organizations, of critical insights and much needed revenue at a time when monetizing digital content is increasingly difficult due to consumers' general unwillingness to pay subscription fees for these services.[48] This burden falls disproportionately on smaller publishers lacking network effects to entice paid subscribers or alternative revenue strategies, such as event curation.[49]

---

see Beales, Howard & Eisenach, Jeffrey, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, Navigant Economics (2014), 10.2139/ssrn.2421405 (finding that absent cookies, ad revenue decreased by more than 66 percent based on a study of impression level data and observations of display ad placements for the top 4000 publishers);
see Goldfarb & Tucker, *Privacy Regulation and Online Advertising*, Management Science (2011), https://econpapers.repec.org/article/inmormnsc/v_3a57_3ay_3a2011_3ai_3a1_3ap_3a57-71.htm (finding that ad prices were 65 percent less effective based on an analysis of responses from 3.3 million survey takers randomly exposed to 9,596 online display advertising campaigns).

[43] *See* Ravichandran & Korula, *supra* note 41.

[44] *See* Goldfarb & Tucker, *supra* note 41; *see also* Ravichandran & Korula, *supra* note 41.

[45] *See* Eisenach & Beales, *supra* note 41 at 13.

[46] Marotta, Abhishek, & Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, Working Paper (2019) (finding that absent cookies, ad revenue decreased by four percent based on a study of a publisher).

[47] *See* Garret Johnson, Comment Letter on Trade Regulation Rule on Commercial Surveillance and Data Security (Oct. 24, 2022), https://www.regulations.gov/comment/FTC-2022-0053-0680.

[48] Competition and Mkt. Auth., *Online Platforms and Digital Advertising: Market Study Final Report*, ¶¶ 2.4-9 (2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study ("The inability of smaller platforms and publishers to access user data creates a significant barrier to entry.")

[49] *See id.* at 61.

As noted above, consumers have consistently been resistant to subscriptions and content paywalls. In 2019, only 16 percent of Americans paid subscription fees for online content. Even among those willing to pay for content, most subscribers only pay for one subscription. However, in the same year, 76 percent of American newspapers established some form of paywall for access to their content.[50] As publishers search for ways to fund themselves, the paywall model suggests a future where consumers have access to less digital content. The marketplace for this content will inevitably become dominated by larger platforms that will rely on vast user bases. Additionally, a paywall-based model serves to keep access to online content away from a large number of consumers, as those willing to pay subscription fees are generally wealthier and more highly educated.[51]

Curtailing the use of tailored advertising would have negative effects across the entire digital media ecosystem, and it would likely have a compound effect on the marketplace, driving many smaller publishers and advertisers out of business while shoring up the market position of the larger and dominant platforms. This would likely also lead to limited options and additional increases in digital ad-pricing on dominant platforms as the only avenue to reach wide and diverse audiences—a likely blow to competition in the industry. We explore the intersection of tailored advertising and digital media competition in greater detail in these comments in section VIII below. Ultimately, the wide range of benefits that tailored advertising provides consumers and businesses alike should be considered by the Commission in any actions it takes related to privacy and digital advertising.

VI. The FTC Should be Guided by Statutory Requirements and Existing Policies that Seek to Ensure Regulations and Enforcement Actions Take into Consideration Costs, Benefits and Market Competition

The NAI agrees with the Commission regarding the importance of protecting consumers from harmful uses of data. However, the ANPR sweeps too broadly and fails to recognize that not all commercial data collection and use is deceptive or unfair. Instead, the ANPR contemplates an expansive perspective on the concerning and ambiguously defined practice of "commercial surveillance." If not explicitly stated, the ANPR suggests and seeks answers to questions suggesting the need to substantially curtail the act or practice of consumer data collection itself, as such collection is inherently too risky and either does, or is likely to lead to, actual harm that warrants an expansive rulemaking.[52] While the ANPR focuses on critical perspectives regarding

[50] *See* Laura Hazard Owen, *Even People Who* Like *Paying for News Usually Only Pay for One Subscription*, NIEMAN LABS (June 11, 2019), https://www.niemanlab.org/2019/06/even-people-who-like-paying-for-news-usually-only-pay-for-one-subscription/.

[51] *Id.*

[52] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51,281 (Question 4, "How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?", Question 7, "How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate its claims of harm or risk of harm?" , Question 11, "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?", and Question 12, " . . .Which commercial surveillance practices, if any, are unlawful such that

the harmful outcomes of commercial data collection and use practices, particularly those pertaining to third-party companies, it is short on evidence of widespread consumer harms.

There is a cognizable difference between, on one hand, reasonable and responsible data collection and processing, first-party and third-party alike, and on the other, practices that are misrepresented, surreptitious, or likely to cause substantial injury without countervailing benefits. There is also a cognizable difference between practices, such as responsible data-driven advertising and marketing that provides consumers–and society as a whole–with tangible benefits, and data collection and processing that lacks countervailing benefits. If the Commission proceeds to propose a rulemaking pertaining to commercial data collection, the NAI urges the Commission to be mindful of the statutory requirements and long-standing policies discussed below that seek to ensure an effective balance between consumer protection, consumer and societal benefit, and marketplace competition.

a. Before Engaging in a Rulemaking, the Commission Must Be Mindful of Section 18's Requirements and Limitations

As the Commission is aware, the Federal Trade Commission Act (15 U.S.C. § 41 *et seq.*) ("FTC Act") provides two avenues for promulgating trade regulations–through either its deception or unfairness authority, or through both. The FTC Act permits the Commission to make rules that define "with *specificity*" unfair or deceptive practices when it "has reason to believe that . . . practices which are the subject of the proposed rulemaking are *prevalent*."[53] To determine if a practice is prevalent, the Commission may look to the existence of cease and desist orders, or when it has "any other information" that "indicates a widespread pattern of unfair or deceptive acts or practices."[54] Additionally, whether the Commission seeks to enhance consumer data privacy by expanding application of its widely used deception authority, or by expanding application of its infrequently used unfairness authority, it should be guided by empirical findings, particularly those practices and harms that are found to be prevalent in the Commission's own enforcement history. Ideally, the Commission would have presented in greater detail in this ANPR how it believes that historical enforcement actions demonstrate the prevalence of unfair and deceptive practices. The NAI encourages the Commission to more thoroughly establish this determination based on enforcement actions if it proceeds with a notice of proposed rulemaking.

i. Unfairness Authority

In determining what constitutes unfair acts or practices for the purpose of pursuing a rulemaking, the FTC must consider whether the practice causes or is likely to cause substantial injury; whether the injury is reasonably avoidable by the consumers themselves; and whether the injury is outweighed by the practice's benefits to consumers or competition.[55] This balancing test and its

new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?").

[53] Fed. Trade Comm'n Act §18, 15 U.S.C. § 57(a).

[54] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51,278.

[55] Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n, and Paul Rand Dixon, Comm'r, Fed.

requirement to take a variety of circumstances into account, has historically guided the Commission with respect to its application of unfairness authority, particularly prohibiting the Commission from seeking to deploy this authority merely for pure policy reasons.[56]

To presume that the collection of consumer data itself is a "substantial injury" for the purposes of the Commission's unfairness authority exceeds the scope of the prescribed statutory balancing test and ignores the numerous benefits to consumers and competition discussed in the previous section of these comments.

The Commission has previously recognized that the majority of legitimate business practices naturally entail a mixture of both costs and benefits; a collection of "tradeoffs" that are inevitable in a vibrant and innovative economy.[57] Therefore, potential minor negative impacts that may accompany activities that provide important societal benefits have correctly not been deemed unfair. Further, the Commission also considers the costs of remedying the purported harm, including to private parties and society at large.

Previous FTC cases are instructive for determining what should and should not be considered an injury for purposes of the unfairness test. Notably, many of the Commission's data breach cases present a comprehensive model of legitimate, substantial harm that is appropriate for potential FTC rulemaking. For example, in 2015, hackers exposed the personal information of more than 30 million AshleyMadison.com users—a website that, among other services, assists married individuals with locating and engaging in extramarital affairs.[58] Hackers misappropriated and published the information of millions, including information about extramarital affairs and infidelity, which led to great personal and public humiliation for many.[59] In addition to reputational harm, two victims of the breach took their own lives as a result.[60] The FTC alleged that the site engaged in unfair business practices that caused substantial consumer harm by failing to take precautions and failing to implement reasonable security measures.[61] For purposes of the FTC Act's balancing test, a scenario such as this presents a clear example of a harm resulting from unfair business practices. One could easily show 1) substantial, demonstrable injury, 2) that the

---

Trade Comm'n, to Wendell H. Ford, Chairman, House Commerce Subcomm. on Commerce, Sci. & Transp. (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [hereinafter Policy Statement on Unfairness].

[56] Fed. Trade Comm'n Act §5(n), 15 U.S.C. §45(n) ("In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.").

[57] *See* Policy Statement on Unfairness ("A seller's failure to present complex technical data on his product may lessen a consumer's ability to choose, for example, but may also reduce the initial price he must pay for the article.").

[58] Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Ruby Corp, No. 1:16-cv-02438 (D.D.C 2016).

[59] Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Ruby Corp, No. 1:16-cv-02438 at 11, (D.D.C 2016).

[60] Laurie Segall, Pastor Outed On Ashley Madison Commits Suicide, CNNBusiness (Sept. 8, 2015), https://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/.

[61] Press Release, Fed. Trade Comm'n, *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach That Exposed 36 Million Users' Profile Information,*(Dec. 14, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting-2015-data-breach-exposed-36-million.

injury was not reasonably avoidable by consumers, who would have had no reason to know the website was insecure, particularly in light of the company's deceptive claims about security, and 3) there was no genuine benefit to consumers or competition to balance out the company's lack of protection.

In the Matter of DesignerWare, the Commission settled charges against seven rent-to-own companies and a software design firm, purporting the companies spied on customers in their homes using rented computers without their knowledge or consent.[62] Through a program called "Detective Mode" DesignerWare maintained the ability to "log [keystrokes], capture screen shots and take photographs using a computer's webcam . . ."[63] revealing scores of personal and highly sensitive information. The FTC also alleged the company made use of geolocation tracking software without obtaining the consent of renters. *DesignerWare* is exemplary of effective application of this test and enforcement authority as intended by the statute and supporting case law[64]–substantial injury occurred in the form of unexpected and disproportionate tracking and gathering of information, the injury was not reasonably avoidable by consumers who did not know of the actions, and the harm to the consumer was not outweighed by the benefit it provided to the respective rent-to-own companies.

In assessing whether the substantial injury in question is outweighed by the practice's benefits, implications to marketplace competition must be considered as well.[65] The Commission staff recently acknowledged that "any approach to privacy must also consider how consumer data fuels innovation and competition[,]" and has warned that "regulation [of data-driven practices] can unreasonably impede market entry or expansion by existing companies."[66] Therefore, in attempting to regulate the data-driven advertising industry, benefits "should be weighed against …potential costs to competition."[67] The Commission has also concluded that consumers benefit immensely from a competitive market, and this sentiment applies particularly to the digital media ecosystem.[68]

As we discuss in greater detail in Section VIII of these comments, the promulgation of broad trade regulations aimed at eliminating third-party data practices would stifle competition in the online ecosystem – placing more power and control in the hands of a few dominant large companies, shutting out small, innovative players, and ultimately harming consumers.

---

[62] Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charged Against Software and Rent-to-Own Companies Accused of Computer Spying (April 15, 2013),https://www.ftc.gov/news-events/news/press-releases/2013/04/ftc-approves-final-order-settling-charges-against-software-rent-own-companies-accused-computer.

[63] *Id*.

[64] *See FTC v. Sperry & Hutchinson Trading Stamp Co.,* 405 U.S. 223, 244-45 (1972).

[65] *See* Policy Statement on Unfairness (To justify a finding of unfairness the injury . . . must not be outweighed by any countervailing benefits to consumers or competition that the practice produces.").

[66] *See* Comment, In re Developing the Administration's Approach to Consumer Privacy, Dckt. No. 180821780-870-01 (Nov. 9, 2018), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf

[67] *Id.*

[68] Fed. Trade Comm'n Bureau of Competition, *Competition Counts How Consumers Win When Businesses Compete*, https://www.ftc.gov/sites/default/files/attachments/competition-counts/zgen01.pdf.

Data from the European Union ("EU") following the enactment of the General Data Protection Regulation ("GDPR") is illustrative of what could happen with respect to digital market competition in the U.S. should the Commission proceed with an overly-broad rulemaking. In a 2020 study, the United Kingdom Competition and Markets Authority found that the EU privacy regulations had substantial detrimental effects on consumers.[69] The GDPR effectuated these harms by increasing the price of goods and services across the economy, reducing competition, imposing unsustainability in the news media, and stifling innovation and development of new services among smaller companies in the market.[70] Based on the current enforcement of the law, larger platforms have both the ability and incentive to interpret data protection regulation in a way that entrenches their own competitive advantage—denying third parties access to data necessary for targeting, attribution, verification and fee/price assessments.[71] Regulation-induced industry consolidation could result in "consumers receiving inadequate compensation for their attention and the use of their personal data by online platforms."[72]

The enforcement of the GDPR ushered in the consolidation of web technology market firms, as there is an apparent inverse relationship between certain privacy regulations and firm consolidation—especially in advertising.[73] One week after GDPR's enforcement, website use of web technology vendors fell by 15 percent for EU residents, and for advertising vendors remained 6 percent below 2018 levels, resulting in significant market consolidation.[74] At the same time, the leading advertising platform's share of the advertising market was found to increase.[75] Concurrently, websites reduced the number of third-party domains requested after the GDPR became effective.[76] In the 18 months following the GDPR, less-popular websites lost more total visits, around a 10-21 percent decrease, than more-popular websites, which experienced a 2-9 percent decrease, further suggesting that the GDPR increases market concentration.[77] This presents a tale of contrasting marketplaces for the time being. On one hand, the stricter GDPR led to a subsequent concentration of the digital advertising market within the European Union among the two largest companies.[78] On the other, we see the digital advertising market within the United States is becoming more competitive as the two largest digital advertising companies are actually declining in market share.[79]

---

[69] United Kingdom Competition & Markets Authority, *Online Platforms and Digital Advertising Market Study* (2020).

[70] *Id.* at 7–12.

[71] *Id.* at 16.

[72] *Id.* at 8.

[73] Garrett Johnson et al., *Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR*, No. 3477686 (Sep. 2022).

[74] *See id.* at 1–2.

[75] *See* Christian Peukert et al., *Regulatory Spillovers and Data Governance: Evidence from the GDPR*, 41 Mark. Sci. 746–68 (INFORMS Jul. 2022).

[76] *See id.*

[77] Julia Schmitt et al., *The Impact of Privacy Laws on Online User Behavior*, No. arXiv:2101.11366, 6 (arXiv Oct. 2021).

[78] *See generally id.*

[79] *See* Max Willens, *US Ad Spending 2022*, INSIDER Intelligence (May 18, 2022), https://www.insiderintelligence.com/content/meta-google-s-hold-on-digital-advertising-loosens-tiktok-others-gain-share.

While the marketplace is continually evolving in the wake of the GDPR and other new privacy regulations, and practices vary across the digital media ecosystem, there is little doubt that privacy regulations can have unintended consequences on market competition if not applied effectively. This is not to suggest that privacy laws and regulations should be avoided entirely, but rather they should be crafted and applied thoughtfully, with a greater focus on retaining current benefits to consumers, and to protect small and medium-sized companies to maximize competition.

Ultimately, before potentially seeking to expand the interpretation of its unfairness authority, the Commission must consider not only whether a substantial injury exists, but also the harm to consumers and the competitive market that would result from such policies. This research suggests that the ability of publishers and other digital media providers to partner with third-party data partners to help offset the inherent market advantages of large first-party platforms–that already account for the lion's share of digital advertising revenue – would be significantly disadvantaged.[80] The NAI therefore urges the Commission to instead focus more precisely on the harmful uses of data it seeks to protect against, and how to bolster data stewardship across all of industry, rather than seeking to limit sharing among partners for advertising and marketing.

ii. Deception Authority

The Commission has traditionally relied heavily on its deception authority, and it has proven to be a very effective regulator in cases where three elements are present – 1) a material representation, omission or practice that is, 2) likely to mislead a consumer, 3) who is acting reasonably based on the circumstances.[81]

The ANPR contemplates the potential areas in which the Commission may use its deception authority to engage in rulemaking, and whether this is an effective approach.[82] The NAI believes that there is continued value in the Commission's deception authority, however, we urge the Commission to consider bolstering its efforts in this area by creating guidance regarding privacy policies and notice/transparency requirements instead of through a lengthy rulemaking process. As we explain in greater detail below in these comments, we believe there are significant opportunities for the Commission to more clearly provide direction to businesses about ways to improve the effectiveness of transparency and control for consumers, buttressed by the Commission's enforcement authority against actors who fail to comply with their commitments.

The ANPR also specifically suggests leveraging this authority to regulate "dark patterns," or practices that deceive or mislead consumers into providing personal information without fair

---

[80] *Id.*

[81] Letter from James C. Miller III, Fed. Trade Comm'n Chairman, to John D. Dingell, Chairman, House Comm. on Energy and Commerce (Oct. 14, 1983) [hereinafter Policy Statement on Deception]. The Policy Statement on Deception is also appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984).

[82] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. at Reg. 51,282 (Question 30, Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extralegal measures, including self-regulation, sufficient? To what extent, if at all, are self-regulatory principles effective?" and Question 31 "Should the Commission commence a Section 18 rulemaking on data security? The Commission specifically seeks comment on how potential new trade regulation rules could require or help incentivize reasonable data security.").

notice and meaningful choice.[83] While we strongly support limiting or restricting the use of unclear or misleading interfaces that pertain to consumer data collection, the NAI encourages the Commission to adhere to the critical analysis it developed to steer this authority, both in future enforcement actions and potential future rulemaking. Principally, the Commission must ensure that the misrepresentation is material—that is, the "practice is one which is likely to affect a consumer's choice of or conduct regarding a product."[84] Second, the practice must be likely to mislead a consumer. Finally, the Commission must impose a "reasonable consumer: standard, and has noted that, "[a] company is not liable for every interpretation or action by a consumer . . ." but rather, the FTC must look at the totality of the circumstances when determining reasonableness.[85] The NAI submitted comments to the FTC in advance of its March 2021 workshop on dark patterns, where we supported the Commission's goal of highlighting and discouraging manipulative and deceptive user interfaces, while also cautioning against that the Commission to avoid prescriptive new regulations, and to increase education and promote best-practices, while enforcing aggressively within the authority granted to the Commission.[86]

VI. The Commission Should Take Practical Steps to Bolster the Role of Transparency and Consumer Control, Not Abandon the Approach as Completely Ineffective

The ANPR inquires about instances where transparency and disclosure requirements are effective for purposes of mitigating consumer harm.[87] When implemented properly and backed by clear and consistent legal requirements, transparency and control requirements can play an extremely valuable role in consumer education, empowerment, and data protection. The NAI continues to believe that it is the role of Congress to provide a national privacy framework to establish consistent standards for transparency, control and accountability across the entire industry. However, until enactment of such a law, the NAI encourages the Commision to fortify the role of transparency and control through an open stakeholder process through which it can explore a range of practices, with the goal to develop clear guidance in this area. This approach can bolster the Commission's enforcement authority,[88] rather than denouncing this framework as ineffective and obsolete,[89] and establishing broad rules seeking to restrict data collection and use.

---

[83] Id. at 51,280.

[84] *See* Policy Statement on Deception, *supra* note 81.

[85] *See id.*

[86] The NAI, Comment on Bringing Dark Patterns to Light: An FTC Workshop (March 15, 2021), https://thenai.org/wp-content/uploads/2021/07/15march2021.pdf

[87] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51,285 (Question 84, "In which contexts are transparency or disclosure requirements effective? In which contexts are they less effective?" and Question 90, "Should new rules, if promulgated, require plain-spoken explanations? How effective could such explanations be, no matter how plain? To what extent, if at all, should new rules detail such requirements?").

[88] *See* id. at 51,282 (Question 31, "Should the Commission commence a Section 18 rulemaking on data security? The Commission specifically seeks comment on how potential new trade regulation rules could require or help incentivize reasonable data security."); *See* id. at 51285 (Question 85, "Which, if any, mechanisms should the Commission use to require or incentivize companies to be forthcoming? Which, if any, mechanisms should the Commission use to verify the sufficiency, accuracy, or authenticity of the information that companies provide?").

[89] See *id*. at 51,275 ("Many consumers do not have the time to review lengthy privacy notices for each of their devices, applications, websites, or services, let alone the periodic updates to them. If consumers do not have meaningful access to this information, they cannot make informed decisions about the costs and benefits of using different services.").

The NAI concurs with others who have recognized that transparency and control continues to have substantial value for consumer protection, but these tools must be applied more effectively, particularly to reflect the current digital media landscape.[90] We recognize the inadequacy of relying on transparency and control mechanisms as a singular means for consumers to protect their own privacy, and the potential for "consent fatigue" resulting from over-reliance on this approach.[91] However, both long-form privacy policies and more concise "just-in-time" privacy notices and choice mechanisms play a valuable role in enhancing privacy and data protection for consumers. Short form notices, such as those promoted by the NAI in our 2020 Code and subsequent guidance, can help consumers compare products and services and make informed decisions based on data collection and use practices. They have also been adopted by leading technology companies and support increasing consumer awareness. Longer privacy policies, while difficult to digest for average consumers, remain valuable tools for regulators, self-regulatory organizations, and privacy watchdogs to assess data collection and use practices by businesses, and hold companies accountable and ensure compliance with these commitments.

Conversely, the ANPR incorrectly asserts that this approach cannot provide privacy benefits, and that various recent legal frameworks have moved *away* from transparency and control.[92] Not only is notice and choice one of the key legal bases provided under the GDPR, but it is also at the core of the five comprehensive state consumer privacy laws enacted over the last several years. All of these state laws, while also providing duties and data minimization requirements for businesses, create new requirements for enhanced transparency and consumer choice, in a consistent effort to enable consumers to better control the collection and use of their data.

As discussed in these comments above, the NAI has long been a leader in setting voluntary industry standards for members with respect to increasing transparency about data collection, and by ensuring that choices are available to consumers. Our 2019 Guidance on Opt-In Consent explains how members should provide detailed just-in-time notice when using opted-in data for Tailored Advertising or Ad Delivery and Reporting (ADR), explicitly requiring companies to provide consumers additional details about the use of their sensitive data for advertising and marketing use cases before they consent.[93] Since this requirement came into effect for NAI members and their partners in 2020, adoption has been growing. However, given that these are still viewed by some

---

[90] *See* Richard Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, J. High Tech. L. (2013); *See also* Jen King et al., *Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interact*, World Economic Forum, 1, 26 (July 2020).

[91] Luis Alberto Montezum & Tara Tauman-Bassirian, *How to Avoid Consent Fatigue*, IAPP (Jan. 29, 2019), https://iapp.org/news/a/how-to-avoid-consent-fatigue/.

[92] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51,276 ("Many [states and countries] accordingly have enacted laws and regulations that impose restrictions on companies' collection, use, analysis, retention, transfer, sharing, and sale or other monetization of consumer data. In recognition of the complexity and opacity of commercial surveillance practices today, such laws have reduced the emphasis on providing notice and obtaining consent and have instead stressed additional privacy "defaults" as well as increased accountability for businesses and restrictions on certain practices.")

[93] Network Advertising Initiative, Guidance for NAI Members: Opt-In Consent (Nov. 2019), https://thenai.org/wp-content/uploads/2021/07/nai_optinconsent-guidance19.pdf.

businesses as voluntary, the FTC could help clarify that other U.S. regulators have determined this to be necessary.[94]

Additionally, in 2020, the NAI published a set of Best Practices for Nonmarketing Uses of Consumer Information, proposing broadly for industry to adopt similar requirements to use cases beyond advertising and marketing uses not covered by our Code of Conduct.[95] These Best Practices were produced with a specific emphasis on sensitive information, as the NAI recognizes that the use of this data poses greater risk of harm. This document establishes that companies can reasonably be expected to apply a materiality test to determine whether their processing—or sharing with partners for processing—of a consumer's data should be disclosed in the just-in-time notices provided to consumers before they consent to share this data. The NAI follows the FTC's guidance on what constitutes a "material" consideration: "The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service."[96] Our Best Practices provide hypothetical scenarios in which a company may determine that the sharing of data is material and therefore discloses that in a just-in-time notice.

The NAI continually seeks to promote practices that not only meet current legal requirements, but, as discussed above, extend beyond these requirements in many cases. However, as discussed above in these comments, self-regulatory efforts have limitations, only extending to companies who choose to adopt them.

The NAI would support FTC efforts to more effectively promote broad and consistent guidance for transparency and control for the collection and processing of consumer data, particularly sensitive data or practices that are likely to affect the consumer's conduct or decision with regard to a product or service. We believe our Code, guidance and best practices for non-marketing uses of data are consistent with consumers' expectations, and that the FTC could promote a similar set of practices through outreach to businesses and policy initiatives, without expending resources on a long, arduous rulemaking process. It should remain a critical priority for the Commission to help consumers more effectively assess and compare digital media services against others based on greater knowledge of how their data will be used. The NAI welcomes the opportunity to continue engaging with the Commission in such an effort.

VIII. Third-Party Businesses Provide an Essential Role in Enhancing Competition Across the Digital Media Ecosystem

Third-party data companies are essential to the competitive digital marketplace, particularly providing benefits for the smallest publishers and advertisers in the ecosystem, and have not been

[94] Press Release, The NAI, NAI Praises L.A. City Attorney's Settlement Over The Weather Channel App (Aug. 10, 2020), https://thenai.org/wp-content/uploads/2021/07/PR08192020.pdf (The Weather Channel used the location tracking technology present in its app to monitor where users live, work, and visit and shared that information with third parties without consent. The NAI strictly prohibits practices such as this, and requires businesses to obtain opt-in consent before using a consumer's location information in this way).

[95] Network Advertising Initiative, Best Practices: Using Information Collected for Tailored Advertising or Ad Delivery and Reporting for Non-Marketing Purposes (June 2022), https://thenai.org/wp-content/uploads/2021/07/nai_nonmarketing-bestpractices-0620_final-1.pdf.

[96] *See* Policy Statement on Deception, *supra* note 81.

proven to present greater risk to consumers. Instead of seeking to dictate the digital media marketplace by minimizing the role of third-party companies, the Commission should work to prevent harmful outcomes of consumer data processing, by first-party and third-party companies alike.

The ANPR raises questions about the distinction between first and third-party companies, suggesting that third-party companies present an increased risk of harm.[97] This was also a substantial topic of discussion at the FTC's stakeholder forum on September 8, 2022.[98] It was suggested by multiple participants in the workshop that the distinction between whether a consumer directly engages with a company should guide the development of a new policy framework that provides broad latitude of those first party companies, and strict limitations on third parties–these remarks of course came from participants representing industry groups of large, first-party businesses with much to gain from a marketplace that disadvantages smaller players with less customers.

In addition to the considerations highlighted above about the need to balance consider the impacts of future enforcement and a potential rulemaking on marketplace competition, we urge the Commission to more thoroughly assess potential distinctions between companies depending on where they sit in the marketplace, particularly taking into consideration the following critical points.

First, these arguments often conflate various uses of data, and harmful or unexpected outcomes of those uses, with the entities that are collecting, storing or processing the data. That is, while there is broad agreement that unexpected and harmful uses of consumer data should be avoided, there are no guarantees, nor any evidence that has been presented to date, that first-party companies have historically been better stewards of consumer data overall than third parties. Nor is there any reason for there to be an inherent reality across the ecosystem that consumers are surprised or harmed when first-party companies they interact with share this data with service providers and third-party partners. As recent examples have shown, it is entirely possible for first-party technology intermediaries touting enhanced privacy to relinquish their commitment when establishing conglomerate market dominance. Indeed, it should be the goal of policymakers broadly, including but not limited to the Commission, to promote policy frameworks that apply protections and enforcement consistently.

Second, these third-party companies provide an essential net benefit for competition across the digital media marketplace, providing opportunities for the smallest publishers and advertisers to compete with the largest internet platforms. At the core of the current digital advertising marketplace, publishers and advertisers often partner with service providers and third-party

---

[97] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51,274 ("[m]ost consumers, for example, know little about the data brokers and third parties who collect and trade consumer data or build consumer profiles that can expose intimate details about their lives and, in the wrong hands, could expose unsuspecting people to future harm.").

[98] *See generally* Fed. Trade Comm'n, Commercial Surveillance and Data Security Public Forum (Sept. 8, 2022), comments from Jason Kint, Digital Content Next, and Paul Martino, National Retail Federation, https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.

companies, including but not limited to ad-tech companies like NAI members, who specialize in helping to tailor and serve ads, and to help measure and increase the effectiveness of these ads.

The largest digital platforms, digital publishers, and retail businesses want to leverage their large customer bases, and the data that accompanies them, not only to enhance their product and service offerings, but also to provide valuable tailored advertising and marketing based on their knowledge of customer preferences. For example, Apple's earnings from advertising increased significantly following updates to its operating system in 2021that limited the amount of information users could share with third-party advertising companies.[99] Apple has since become subject to litigation for misleading its customers by providing "privacy controls" that ultimately make it more difficult for consumers to opt-out of Apple's *own* data collection across their own platform and services, for their use to customize content, advertising and marketing.[100] Essentially, after erecting policies and controls that substantially discourage consumers from sharing their data with other app publishers and their partners, Apple leveraged its own role as a market dominant technology provider—across multiple technology platforms and digital content services—to perform similar practices with limited transparency and control.

Smaller businesses, particularly smaller digital businesses such as the D2C companies we discuss above, lack these large customer bases and would be ill equipped to compete in an environment where they could not rely on data sharing with third-party partners to compete with those larger businesses. Unfortunately, these smaller businesses are not adequately represented in public policy discussions about consumer privacy and marketplace competition, and their perspectives are ultimately drowned out by these larger businesses.

As the Commission and other global competition regulators have identified over the last several years, it is essential to maintain robust competition across the digital media ecosystem, particularly the marketplace for digital advertising. Given that the largest digital platforms currently maintain inherent advantages in providing digital advertising,[101] the Commission should more appropriately focus on the uses of consumer data, and particularly the outcomes and consumer harms that should be avoided.

IX. Conclusion

Again, thank you for the opportunity to comment on this important issue. We look forward to the opportunity to continue working with the Commission as you move forward with all efforts to enhance consumer data privacy and security.

---

[99] *See* Mark Gurman, *Apple Finds Its Next Big Business: Showing Ads On Your Phone*, Bloomberg (Aug. 14, 2022), https://www.bloomberg.com/news/newsletters/2022-08-14/apple-aapl-set-to-expand-advertising-bringing-ads-to-maps-tv-and-books-apps-l6tdqqmg.

[100] *See* Matt Binder, *Apple Sued for Tracking Users' Activity Even When Turned Off in Settings*, Mashable (Nov. 12, 2022), https://mashable.com/article/apple-data-privacy-collection-lawsuit.

[101] See *US Ad Spending 2022, supra* note 79.