409 7th Street, NW Suite 250
Washington, DC 20004

March 6, 2023

Travis Hall
Policy Specialist
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW; Room 4725
Washington, DC 20230

Dear Mr. Hall,

On behalf of the Network Advertising Initiative (NAI), thank you for the opportunity to provide comments on the National Telecommunications and Information Administration ("NTIA") Request for Comment ("RFC") on the intersection of privacy, equity, and civil rights.[1]

I. Introduction

A. Overview of the NAI

Founded in 2000, the NAI is the leading non-profit, self-regulatory association for advertising technology companies. For over 20 years the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining and enforcing the highest industry standards for the responsible collection and use of consumer data. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and enhancing consumer trust. As a non-profit organization, the NAI promotes the health of the digital media ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising across all digital media.

All NAI members are required to adhere to the NAI's FIPPs-based,[2] privacy-protective Code of Conduct (the "NAI Code"), which continues to evolve and recently underwent a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy.[3] The NAI continues to monitor state and federal legal and regulatory changes, and our Code evolves to reflect–and in some cases exceed–those requirements. Member compliance with the NAI Code is promoted by a strong accountability program. NAI attorneys subject each NAI member to a comprehensive annual review of

[1] National Telecommunications and Information Administration Privacy, Equity, and Civil Rights Request for Comment, 88 Fed. Reg. 3714 (proposed Jan. 20, 2023).
[2] *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.
[3] *See* NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter "NAI Code"], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

their businesses and data collection and use practices for adherence to the NAI Code. In addition, NAI staff advises companies on an ongoing basis about how to best comply with the Code and guidance and how to implement privacy-first practices. Finally, the NAI team conducts technical monitoring and review of company opt outs and privacy tools. Enforcement of the NAI Code can include penalties for material violations, and potential referral to the Federal Trade Commission ("FTC"). Annual reviews cover member companies' business models, privacy policies and practices, and consumer-choice mechanisms.

B. Summary of NAI Comments and Recommendations

The NAI believes that maintaining a robust, ad-supported digital media ecosystem is not in conflict with the objective of increasing privacy, enhancing protections for civil rights, and avoiding harmful outcomes. While we provide answers to many of the specific questions raised in the RFC below, following are key recommendations for the NTIA as the agency develops a report and proposes solutions:

1. Promote a national privacy law to provide uniform protections for consumers across the United States, limit unreasonable and harmful outcomes, and to provide a consistent set of requirements for businesses that process personal information.
2. Recommend standard practices for data protection assessments to addresses disparate impacts and harmful outcomes to protected classes and the underserved, and to harmonize compliance with the distinct state law requirements to the greatest extent possible.
3. Promote the role of self-regulatory efforts to mitigate bias and discrimination resulting from automated decision making, and convene a dialogue among key stakeholders to promote collaboration in the development of common objectives and practices.
4. Review existing civil rights laws to assess gaps in their application across the digital media ecosystem, and recommend amendments if necessary.

II. Framing

This section explores how regulators, legislators and other industry stakeholders should approach civil rights and equity implications of commercial data collection and processing. Importantly, the question is raised about whether "privacy" is the best term to discuss these issues. The NAI does not believe that this is inherently a discussion of privacy. Rather it is more accurately a discussion of policies, practices, and most importantly outcomes, pertaining to the processing of personal information. Below are responses to some key questions raised in this section that we hope will help to better frame the NTIA's efforts to combat discrimination and disparate impacts of data processing, and preserve essential civil rights.

- ***Q1(c): How should discussions of privacy and fairness in automated decision-making approach the concepts of "sensitive" information and "non-sensitive" information, and the different kinds of privacy harms made possible by each?***

For many years, the NAI has maintained the highest industry standard for defining and protecting sensitive data categories, for which we require opt-in consent for the use of such data for advertising and marketing purposes. The NAI has always tried to differentiate between sensitive and non-sensitive information in a way that both protects truly sensitive information while at the same time not casting so wide a net as to render all information sensitive and prevent its collection. The NAI's definition of

sensitive information focuses on certain medical conditions (e.g., all types of cancer, mental health conditions, sexually transmitted diseases, or conditions primarily affecting children not treatable by over-the-counter medication) as well as information (including inferences) about a consumer's sexual orientation,[4] and it also includes the types of data that are increasingly being collected through mobile phones and connected devices, such as sensor data, and personal directory data that consumers enter or compile on their own devices.

As Professor Daniel Solove notes, the harms of processing sensitive data arise not from processing sensitive data *per se*, but by *how* that data is processed and utilized.[5] Non-sensitive data can be used in such a way that causes the same harm that sensitive data processing has been thought to produce, while some instances of processing sensitive data actually benefit the marginalized groups and broader society.[6] The focus therefore should shift from classifying and regulating sensitive versus non-sensitive data, and instead to regulating harmful uses of data while promoting beneficial uses of data.[7] Such a regime where the law, for example, would categorize types of harm instead of data,[8] would more efficiently and effectively prevent harms from data use while promoting good uses of data,[9] prevent entities from using privacy law as a pretext to attack competition,[10] and prevent inadvertently undermining the protection of marginalized communities which need to be able to process sensitive data.[11] In other words, a functionalist, outcome-based approach better protects the civil liberties and rights of consumers while the current typological system abjectly fails to do so.

While the NAI definition of sensitive data largely aligns with the definition established by the multiple new U.S. state privacy laws, there are some categories of data where we diverge, notably the state legal requirements that consider information about a consumer's race or ethnicity to be sensitive.[12] We recognize and agree that many consumers have increased sensitivity around these data types, and that they could present an increased likelihood of leading to disparate outcomes, particularly if processed for purposes such as eligibility determinations. For this reason, the NAI prohibits the use of any data collected for advertising and marketing to be used for eligibility determinations.[13] This approach preserves the ability of companies to tailor advertising based on these categories, and it places restrictions on companies who the data is shared with, further mitigating the potential for harmful outcomes.

However, there are many cases where demographic data such as race and ethnicity can be utilized to reach at-risk communities and promote products and services that are beneficial to these populations. For instance, tailored advertising was recently deployed by health organizations to reach at-risk

[4] NAI Code § I.O (2020).
[5] Daniel Solove, *Data is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. __, 18 (forthcoming 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.
[6] *Id.* at 41–45.
[7] *Id.*
[8] *Id.* at 46.
[9] *Id.*
[10] *Id.* at 47.
[11] *Id.*
[12] *See, e.g.*, Cal. Civ. Code § 1798.140(ae)(1)(D) (2023) (definition of "sensitive personal information" to include "[a] consumer's racial or ethnic origin").
[13] *See* NAI Code § II.D.2 (2020).

populations and educate them about the value of COVID vaccines.[14] Advertising for educational institutions and services is another key area where identification of these data types can have beneficial outcomes, such as promoting racial or ethnic diversity. There are myriad other opportunities to use data to encourage inclusion, rather than to discriminate, and these practices should be actively encouraged and aided.

NTIA's consideration of privacy and fairness in automated consumer data processing should therefore focus on how to identify and regulate the resulting impact from certain processing activities, instead of seeking to limit data collection and processing broadly or based on an expansive set of "sensitive information." The NAI encourages the NTIA to fully recognize the beneficial uses of data, including that which could be considered "sensitive," and to craft rules that do not unnecessarily limit the collection and use of data broadly, and to preserve opportunities to benefit protected classes and at-risk populations. As we discuss below, the requirements for businesses to conduct data protection assessments ("DPAs") is crucial in helping to determine processing that poses a heightened risk of harm to a consumer, and to identify whether the risks outweigh the benefits.

- ***Q1(d): How should the individual and collective natures of privacy be understood, both in terms of the value of privacy protections; the harms of privacy invasions; and the implications of those values and harms for underserved or marginalized communities?***

This question, and the context leading up to it, focuses heavily on "privacy invasions," or the harms that come from the misuse of personal information. However, there is not significant consideration conversely about the benefits that society derives from innovative uses of data, and particularly uses that promote inclusion and opportunities to underserved populations. The NAI recommends that the NTIA further explore benefits that can derive from data collection, and how to encourage beneficial uses of data, rather than overly focusing on harms associated with data collection and processing, particularly automated decision making. One of the most basic examples of benefits to underserved communities are the free and low-cost services that comprise the bulk of the digital media ecosystem. If these services are delivered without significant harmful outcomes, they are a tremendous benefit. Conversely, overly focusing on "privacy," and seeking to limit data collection, is likely to lead to a change in the marketplace for digital media products and services, where there are "haves," and "have nots." In the effort to prevent data harms and promote "privacy," over reliance on trying to establish a preconceived notion of privacy expectations is unhelpful.

III. Impact of data collection and processing on marginalized groups

This section explores important questions about disproportionate harms, particularly with respect to data collected or processed in the context of evaluation for credit; healthcare; employment or evaluation for potential employment; education or educational opportunities; and housing and evaluation for housing; insurance, and evaluation for insurance. As the NTIA rightly notes in its RFC, marginalized and underserved communities are especially vulnerable to privacy violations, and that specific data collection and use practices can potentially create or reinforce discriminatory obstacles for marginalized groups regarding access to key opportunities, such as employment, housing, education, health care, and access to credit.

[14] Dan Diamond, *It's Up to You: Ad Campaign to Encourage Coronavirus Vaccinations Get Underway*, THE WASH. POST, (Feb. 25, 2021), https://www.washingtonpost.com/health/2021/02/25/covid-vaccine-ad-council/.

The NAI recognizes these realities and we are proud to be an industry leader in prohibiting our members from the secondary use of information collected for tailored advertising for certain eligibility purposes, including credit, insurance, housing, and education as discussed above. This prohibition applies regardless of whether such information is ever sold, and even when a consumer has not opted out of tailored advertising.

- ***Q3(c): When should particular types of data be considered proxies for constitutionally-protected traits? For example, location data is frequently collected and used, but where someone lives can also closely align with race and ethnicity. In what circumstances should use of location data be considered intertwined with protected characteristics? Are there other types of data that present similar risks?***

In June 2022, the NAI published Precise Location Information Provider Voluntary Enhanced Standards ("Enhanced Standards").[15] This set of guidelines for companies that collect consumer location information restricts the use, sale, or transfer of location data correlating to certain sensitive points of interest, including places tied to religious worship, sensitive health care services, military bases, and LGBTQ+ identity, among others. These standards would prohibit, for instance, both the processing and transfer of information on an individual consumer's visit to a Planned Parenthood clinic, or to a Jewish synagogue, or to a gay bar. The standards protect consumer privacy while also allowing for participants to continue to do business and help fund the internet.

Notwithstanding the criticisms of a typified approach to sensitive data as discussed above, in our own work as a self-regulatory body, the NAI has tried to strike a balance between having meaningful protections in place for sensitive data and not defining the term so broadly that all data is effectively rendered sensitive. For example, with our Enhanced Standards, we differentiated between raw location data (*e.g.*, latitude and longitude coordinates) and the context of certain points of interest. By itself, location information means very little without the context of the points of interest; consequently, the NAI's Enhanced Standards prohibit participants from passing the *contextual* information to their clients and other downstream market participants. For example, this allows instances where a sensitive point of interest (such as a reproductive health center) is in close proximity and virtually indistinguishable from a non-sensitive point of interest (such as a fast food restaurant).

IV. Existing Privacy and Civil Rights Laws

Although modern data uses may present new means for bad actors to discriminate, underlying discrimination itself cannot be reduced to a matter of mere data collection alone, and several legal tools are already at enforcers' disposal to prevent and deter uses of data that result in illegal discrimination. We encourage NTIA to promote more effective enforcement of existing civil rights statutes to address potential discrimination through the collection and processing of data.

Congress has enacted several laws that protect consumers from misuses of data that have the effect of illegal discrimination or civil rights violations, some dating back nearly half a century. Examples include

[15] NETWORK ADVERTISING INITIATIVE, *NAI Precise Location Information Solution Provider Voluntary Enhanced Standards* (June 22, 2022), https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/#:~:text=The%20Enhanced%20Standards%20create%20restrictions,LGBTQ%2B%20identity%2C%20and%20other%20places.

the Civil Rights Act of 1964; the Fair Housing Act, the Fair Credit Reporting Act; the Equal Credit Opportunity Act; and the Americans with Disabilities Act; among others.[16] Another example of current law with substantially applicability is the FTC Act, which provides for enforcement and relief related to unfair and deceptive practices that may result in civil rights violations or illegal discrimination.[17] The FTC recently highlighted the application of these statutes in a warning to industry about potential discriminatory outcomes from automated decision making.[18] The Consumer Financial Protection Bureau ("CFPB") also recently issued an interpretive rule laying out how digital marketers for financial firms must comply with federal consumer financial protection law.[19] Under the CFPB's interpretation, because a digital advertiser selects the audience that will see an advertisement, the digital advertiser is considered a service provider under the Consumer Financial Protection Act of 2010 and can be held liable under that Act for unfair, deceptive, or abusive acts or practices.[20] As reflected by their compliance warnings, both the FTC and CFPB are applying new interpretations of these long-standing laws. While these laws apply clearly in some cases to modern data processing, in other cases there is ambiguity about their application and the interpretation of regulatory agencies that could benefit from analysis by the NTIA.

- **Q4(f):** ***Legislators around the country and across the globe have enacted or amended a number of laws intended to deter, prevent, and remedy privacy harms. Which, if any, of these laws might serve as useful models, either in whole or in part? Are there approaches to be avoided? How, if at all, do these laws address the privacy needs and vulnerabilities of underserved or marginalized communities?***

As discussed in Section V of these comments below, the NAI believes that the requirements for data protection assessments will prove instrumental in the effort to combat discrimination and disparate impacts that can result from processing of personal information. Additionally, as discussed above in Section II, the NAI strongly urges the NTIA to refrain from an overly broad focus on sensitive information that could be the outcome of ambiguous definitions of "sensitive personal information" as defined in multiple new state consumer privacy laws. Instead, we encourage the NTIA's consideration of privacy and fairness in automated consumer data processing to center around how to identify and prevent any harmful resulting impact from certain processing activities.

---

[16] *See, e.g.,* Civil Rights Act of 1964, 42 U.S.C. § 2000d *et seq.*; Fair Housing Act, 42 U.S.C. § 3601 *et seq.*; Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; Equal Credit Opportunity Act, 15 U.S.C. § 1691 *et seq.*; Americans with Disabilities Act, 42 U.S.C. § 12101 *et seq.*

[17] FTC Act, 15 U.S.C. § 45.

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

[19] Press Release, Consumer Fin. Prot. Bureau, *CFBP Warns that Digital Marketing Providers Must Comply with Federal Consumer Finance Protections* (Aug. 10, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-that-digital-marketing-providers-must-comply-with-federal-consumer-finance-protections/.

[20] *Id*.

V. Solutions & Other Actions

Despite decades of strong accomplishments in enhancing privacy protections for consumers around the collection and processing of data for digital advertising, there are obvious limits to self-regulation in the absence of uniform, clear legal requirements. Self-regulation increasingly guides the best-intentioned companies, but it also requires them to compete with others who maintain lower standards, without sufficient competition on privacy standards across the marketplace. Without a uniform national framework in place, the good actors will behave responsibly, but bad actors will continue to misuse consumer data in ways not protected by the patchwork of current federal and state privacy laws. While citizens in some states will benefit from new privacy laws, citizens in other states will not be assured the same protections. The growing patchwork of state privacy laws is a well-intentioned stopgap, but it is neither in the best interest of consumers nor businesses. For this reason, the NAI supports a federal privacy law to establish a uniform framework for businesses collecting and processing personal information in the United States. An effective law should focus primarily on outcomes, with protections against unexpected and harmful outcomes of data processing, rather than broad bans on data collection and use, which is impractical and undesirable. The NAI is eager to continue working with the NTIA and other federal policymakers, industry stakeholders, and civil society, in developing workable standards that protect consumers and allow for a vibrant, functioning digital economy.

- ***Q5: What are the principles that should guide the Administration in addressing disproportionate harms experienced by underserved or marginalized groups due to commercial data collection, processing, and sharing?***

The NAI strongly believes that consumer-friendly privacy-protective practices and regulations are not contrary to the business needs of the digital advertising industry. For over twenty years, our industry self-regulation has sought to guide our member companies in the direction of responsible data stewardship. Building on this, any new privacy-focused regulations must make a meaningful difference to consumers. However, particularly considering the five new state consumer privacy laws, there is an overemphasis on the prevention of "selling" or "sharing" of personal information, rather than focusing on harmful or unintended outcomes from data processing.

When digital advertisers have lost consumer trust, this hurts their relationships with brands and publishers, making the value proposition that digital advertising brings to funding a free and open internet a moot point. When digital advertisers value privacy and put privacy-protective measures in place, both consumers and the industry stand to benefit immensely.

Over time, it is likely that these state laws—and likely similar laws to be enacted over the next several years—will have a disproportionate and anti-competitive effect on the digital marketplace, without sufficiently protecting consumers from misuse of their data by companies that are "first parties." The end result could be that consumers do not get meaningfully new protection from processing by these companies, and that these laws disproportionately, and unintentionally, harm smaller businesses with less consumer data. Instead, new laws, regulations and enforcement should focus on preventing unexpected and harmful outcomes, rather than overly focusing on regulating companies, such as "third-party" businesses because of where they sit in the marketplace and whether their role is well

understood by consumers.

- **Q6(c):** ***What roles should third-party audits and transparency reporting play in public policy responses to harmful data collection and processing, particularly in alleviating harms that are predominately or disproportionately experienced by marginalized communities? What priorities and constraints should such mechanisms be guided by? What are the limitations of those mechanisms? What are some concrete examples that can demonstrate their efficacy or limits?***

DPA's, also commonly referred to as Data Protection Impact Assessments ("DPIAs"), are increasingly recognized as essential practices for various types of data processing. For many years, Europe's General Data Protection Regulation (GDPR) has required the performance of such assessments for data processing that "is likely to result in a high risk to the rights and freedoms of natural persons."[21] The law sets out three categories in which DPIAs are always required: systematic and extensive profiling with significant effects, processing of sensitive data on a large scale, and systematic monitoring of public areas on a large scale.[22]

In addition to these assessments being common practices for companies operating in Europe, similar requirements have also been required by the state laws recently enacted across the United States, with a particular emphasis on processing that presents a heightened risk of harm to consumers, as well as a requirement for companies engaging in data-driven advertising. These assessments are a critical new tool in the effort to combat disparate impacts, as they can be instrumental in identifying and minimizing risks posed by the collection and processing of personal information.

The NAI's long-standing Code and compliance program is in essence a DPA program to identify and minimize risks surrounding the collection and use of consumer data for digital advertising purposes, predating the legal requirements established under the GDPR and newer U.S. state laws. The NAI's compliance team actively works with companies to assess practices, and as these practices evolve and new privacy risks are identified, we regularly update our Code and associated guidance documents, raising the bar to ensure that NAI members are upholding the highest standards among industry.[23] In response to the new state legal requirements for risk assessments around various types of data and practices, the NAI has begun a process of mapping the requirements to digital advertising practices, with the goal to help companies tailor their own assessments building from core NAI compliance requirements as the foundation.

Including and beyond the role of the NAI, third-party auditing organizations can be beneficial for consumers, for industry, and for the government. By allowing trusted, experienced professionals to perform audits, businesses can rely on these third parties to provide clarity in any laws and regulations while also providing benchmarked assessments. When a business is undergoing an audit, as opposed to a formal investigation with law enforcement, the business will speak more candidly about its practices,

---

[21] "Art. 35 GDPR - Data Protection Impact Assessment." GDPR.eu, 23 July 2020, https://gdpr.eu/article-35-impact-assessment/.

[22] "When Is a Data Protection Impact Assessment (DPIA) Required?" European Commission - European Commission, 18 Dec. 2019, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en.

[23] *See* NETWORK ADVERTISING INITIATIVE, *Annual Report* (2021), http://thenai.org/wp-content/uploads/2022/08/2021NAIAnnualReport1.pdf.

allowing the auditing organization to more fully assess the business's practices, and to help the company take steps to correct those practices. The NAI has maintained this model for over twenty years, and we have found that our member organizations trust the NAI to protect their proprietary trade secrets, and they rely on the feedback we provide to them to enhance their data stewardship and come into conformance with both industry and legal requirements.

The new state law requirements for DPA will ultimately help level the playing field, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. Further, the ability of regulators to request access to the results of risk assessments in performing an audit provides enhanced transparency, provided that regulator audits provide essential protections of trade secrets and proprietary practices. With the implementation of multiple state laws and their disparate requirements, businesses are likely to be overwhelmed in their effort to comply efficiently in performance of DPAs.

The NAI believes that while a national privacy law is the ideal approach to establish uniform requirements and criteria for DPAs, in the interim the NTIA should recommend standard practices for DPAs to both harmonize to the greatest extent possible the various state law requirements, and to focus on disparate impacts and harmful outcomes to protected classes and the underserved. We make further recommendations below regarding the goal to leverage existing industry efforts in this effort.

- **Q6(e):** ***What role should industry-developed codes of conduct play in public policy responses to harmful data collection and processing and the disproportionate harms experienced by marginalized communities? What are the limitations of such codes?***

Industry associations have a thorough understanding of common industry practices and are therefore well positioned to develop practical codes of conduct, best practices, and other resources to promote self-regulation that complements, and in the case of the NAI, sometimes extends beyond current legal requirements. As discussed above, the NAI has continually updated our Code over time to adapt to changing industry practices and new challenges that arise in the marketplace. We are currently working to further update our Code and self-regulatory program substantially to bring this in line with new state laws, as well as evolving state and federal regulations, with a key focus on assessing advertising and marketing practices for disparate impacts, particularly because of automated decision making or artificial intelligence (AI).

IBM[24] and the Interactive Advertising Bureau ("IAB")[25] have provided highly distinct initiatives to assist digital advertising companies evaluate AI and automated decision-making systems and protect against biased and harmful outcomes. These programs, while differing in approach, are both technically and operationally sophisticated.

Both the IBM and IAB resources not only recommend auditing, but also propose steps that go beyond simply evaluating whether processing has led to harms after the fact. These industry initiatives recommend auditing not just the algorithm but also, in certain cases, the development process of the

[24] IBM WATSON ADVERTISING, *Advertising Playbook for AI Fairness 360* (2022), https://info.watsonadvertising.ibm.com/rs/765-YGI-327/images/AI%20Fairness%20360.pdf.
[25] INTERACTIVE ADVERTISING BUREAU [hereafter "IAB"], *Understanding Bias in AI for Marketing: A Comprehensive Guide to Avoiding Negative Consequences with Artificial Intelligence* (2021), https://www.iab.com/wp-content/uploads/2021/11/IAB_AI_Bias_Guide_2021-11.pdf.

entire project for harmful bias. The underlying conclusion and core recommendation is that because potentially harmful biases leak into the AI system at all stages of the project lifecycle, discrete checks for the bias and unique ways to clean out that bias at each of those different stages are necessary. In that pursuit, IBM promotes using a toolkit of quantitative techniques to precisely measure for bias, providing different statistical measures for different kinds of biases. IAB presents a more comprehensive set of actions that all of the different stakeholders involved in and/or affected by the AI product should take.

In the case of IBM's initiative, it seeks to implement the principle of "fairness by design,"[26] or the idea that fairness in the form of minimized bias and fair outcomes should be embedded into the AI algorithm at the outset and ensured by continuous monitoring to the end of the AI's lifetime. Of course, a key challenge with seeking to achieve an abstract value such as of fairness is that it does not enjoy common understanding, similar to the concept of privacy, and these do not easily lend themselves to be coded with consistency.[27]

While government agencies such as recently the National Institute of Standards and Technology[28] have called for a similar want of fairness at the design stage, the industry initiatives' level of technical detail and quality of operationalizability provide additional value with particular application to data-driven advertising. These industry initiatives are still new and in an early stage of recognition and adoption across industry, but they are both strong examples of how industry's technological expertise is applied in the context of society facilitating a powerful partnership between self-regulation and governmental regulations.

The NTIA, through its report deriving from this RFC and proposed actionable recommendations, should initiate a dialogue among key stakeholders to evaluate and discuss specific initiatives to mitigate bias and discrimination resulting from processing of personal information and automated decision making, including in advertising and marketing, but also more broadly. Such a process should provide an opportunity for stakeholders to explain and promote their proposed solutions, and to create an inventory of tools, as well as seeking to develop collaboration and iteration among various approaches.

---

[26] IBM, *supra* note 28, at 20; IAB, *supra* note 29, at 17 (although this guidebook does not refer to "fairness by design" by name, its recommendations significantly align with it); *see also* Ahmed Abbasi, Jingjing Li, Gari Clifford, & Herman Taylor, *Make "Fairness by Design" Part of Machine Learning*, HARVARD BUS. REV. (Aug. 1, 2018), https://hbr.org/2018/08/make-fairness-by-design-part-of-machine-learning.

[27] IBM, *supra* note 28, at 14*; compare* ARI WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER, 23 (2021) (noting the complaint widespread among engineers is that privacy is difficult and too fuzzy to "code for"); *see also* Katharina Koerner, *Privacy as Code: A New Taxonomy for Privacy*, INT'L ASSOC. OF PRIVACY PROFS. (Nov. 11, 2021), https://iapp.org/news/a/privacy-as-code-a-new-taxonomy-for-privacy/; Jason Hong, *Why is Privacy So Hard?*, COMMC'N OF THE ASSOC. OF COMPUTING MACHINERY, GEORGETOWN UNIV. (Mar. 13, 2019), https://cacm.acm.org/blogs/blog-cacm/235401-why-is-privacy-so-hard/fulltext; Sarah Spiekermann, *The Challenges of Privacy by Design*, COMMC'N OF THE ASSOC. OF COMPUTING MACHINERY, GEORGETOWN UNIV. (July 2012), https://www.researchgate.net/publication/254004794_The_Challenges_of_Privacy_by_Design.

[28] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

VI. Conclusion

Again, the NAI appreciates the opportunity to submit comments on this important topic. If we can provide any additional information, or otherwise assist the NTIA as it develops a report and recommendations, please do not hesitate to contact me at.

Respectfully Submitted,

David LeDuc
Vice President, Public Policy
Network Advertising Initiative (NAI)