LEADERSHIP AND
MARKETING EXCELLENCE

July 17, 2018

Submitted Via Email: iipp2018@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Attn: Fiona Alexander
Washington, DC 20230

RE: Request for Comment on "International Internet Policy Priorities"

To Whom It May Concern:

On behalf of the Association of National Advertisers ("ANA"), we provide comments in response to the National Telecommunications and Information Administration's ("NTIA") request for public comment on "International Internet Policy Priorities" published on June 5, 2018.[1]

The ANA makes a difference for individuals, brands, and the industry by driving growth, advancing the interests of marketers and promoting and protecting the well-being of the marketing community. Founded in 1910, the ANA provides leadership that advances marketing excellence and shapes the future of the industry. The ANA's membership includes nearly 2,000 companies with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than $400 billion in marketing and advertising annually. The membership is comprised of more than 1,100 client-side marketers and more than 800 marketing service provider members, which include leading marketing data science and technology suppliers, ad agencies, law firms, consultants, and vendors. Further enriching the ecosystem is the work of the nonprofit ANA Educational Foundation, which has the mission of enhancing the understanding of advertising and marketing within the academic and marketing communities.

The NTIA's notice of inquiry seeks comments on NTIA's international internet policy priorities to help NTIA identify priority issues and to assist it in leveraging its resources and expertise to address those issues. We urge NTIA to set as its priority the advocacy and support for strong consumer internet privacy protections at a level that ensures that consumers continue to have access to the full benefits of the internet and that maintains the United States' leadership in the digital economy. ANA members have long supported providing consumers with transparency in data practices, privacy controls, and other privacy protections embodied in the U.S. federal regulatory framework. Consumers also should be able to continue to reap the benefits of free and low-cost online content, products, and services through the ad-supported Internet, which the U.S. federal framework provides.

[1] International Internet Policy Priorities, 83 Fed. Reg. 108, 26036-26038 (June. 5, 2018).

Other jurisdictions, such as the European Union ("EU"), have taken a more restrictive approach to regulating Internet privacy, which threatens the free flow of information online and impacts U.S. businesses and consumers. We recommend that the NTIA carry out a rigorous analysis on the impacts of alternative privacy frameworks such as the EU's General Data Protection Regulation ("GDPR")[2] to determine their effects on competition and consumers. We believe the NTIA will find that laws like the GDPR will limit competition, overburden consumers with opt-in notices and make an efficient and effective digital economy harder to maintain. NTIA should share its findings with international bodies and policymakers considering adopting GDPR-like legislation.

In these comments, we discuss the following topics, which we hope will inform the NTIA's work promoting the continued growth of the internet: 1) the foundational value of advertising and marketing to our society; 2) the benefits of online advertising and marketing to the digital economy; and 3) specific responses to NTIA's questions related to the free-flow of information online and issues related to consumer privacy.

I. The Foundational Value of Advertising and Marketing in American Society

Advertising and marketing occupies a major place in American society. Linked to the bedrock principles that shaped our nation—free speech, competition and individual choice—advertising and marketing have served the public since colonial times as a source of vital information about our open, market-based economy. Advertising and marketing serves to:

- ***Fuel economic growth***. To compete and grow in today's marketplace, companies must efficiently reach consumers, alerting them to new product innovations and competitive price points;

- ***Foster a wide array of affordable media choices***. Vast, affordable media options enrich our society and underpin a core American value: the democratization of knowledge and information; and

- ***Educate the public***. Advertising informs consumers about product choices available in the marketplace.

The goal of advertising and marketing has always been to connect consumers with the products and services they desire, when they desire them. In today's globalizing business landscape, advertising and marketing remain foundational activities for nearly every business, helping businesses provide customized offerings to an ever broader consumer audience. Advertising and marketing also generates employment and business activity throughout the economy. A recent study by IHS, a leading economic consulting firm, found that every direct job in an advertising-defined occupation (*i.e.*, those employed at advertising firms) supported 34 other jobs across a broad range

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR").

of industries throughout the U.S. economy.[3] In addition, every million dollars spent on advertising supported 67 American jobs.[4]

As more and more products and services move online and as consumers increasingly spend time engaging with content on digital platforms, online advertising and marketing will continue its skyrocketing growth path, as will the value that society derives from data-driven advertising and marketing practices.

II. The Benefits of Online Advertising and Marketing to the Digital Economy

Advertising and marketing fuels the digital economy. Every day consumers' lives are enriched by data-driven resources, including an unprecedented array of high-quality information and entertainment. Revenues from online advertising support and facilitate e-commerce, and subsidize the cost of content and services that consumers value and expect, such as online newspapers, blogs, social networking sites, mobile applications, email, and phone services.

Consumers value these ad-supported services and products and benefit from the diversity of companies online. In a recent Zogby survey, over 90% of consumers stated that free content was important to the overall value of the internet, and 75% noted that they prefer content to remain free and supported by advertising rather than pay for ad-free content.[5] Eighty-five percent of consumers surveyed stated they prefer the existing ad-supported model, and 75% also indicated they would greatly decrease their online engagement if the ad-supported internet were to go away. In 2016, a poll revealed that consumers assign a value of almost $1,200 a year to ad-supported online content.[6]

As the data suggests, the current digital economy relies heaving on advertising and marketing to provide consumers the products and services they desire. A study commissioned led by Prof. John Deighton at the Harvard Business School reported that the ad-supported internet ecosystem generated $1.121 trillion for the U.S. economy and was responsible for 10.4 million jobs in the U.S. in 2016.[7] Increasingly, however, the digital economy faces legislative threats and overly prescriptive proposals to regulate the collection and use of data, such as the recently enacted California Consumer Privacy Act of 2018 and the EU's GDPR.[8] (As discussed further in Section III below)

---

[3] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (2015).

[4] *Id*.

[5] Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016), *available at* http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf.

[6] Digital Advertising Alliance, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1,200/Year; 85% Prefer Ad-Supported Internet to Paid*, PR Newswire (May 11, 2016), *available at* http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html.

[7] IAB, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), *available at* https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf.

[8] California Assembly Bill 375; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

To ensure that consumers continue to enjoy online content, products, and services at little to no cost to them, the data that underpins advertising and marketing must continue to be available and overly proscriptive regulatory efforts should be rejected. Strong consumer privacy protections are important and must be balanced with the other benefits of the digital economy that consumers value and expect, including personalized services, seamless product and service offerings, and affordable choices.

III. Responses to Specific NTIA Inquiries

The ANA offers its views on the following specific questions in the NTIA's request for public comment.

a. What are the challenges to the free flow of information online?

The NTIA's notice of inquiry asks for input on the challenges to the free flow of information online. New heavy-handed approaches to the regulation of internet data, including overly proscriptive and broad opt-in consent requirements for the collection, use, and sharing of data, as well as legislation imposing vague consumer data "rights," are some of the most significant challenges to the free flow of information online. Consumers deserve strong internet privacy protections but those protections must be calibrated to a level that ensures that they can continue to have access to the full benefits of the internet.

Over-Regulation of Data. Insufficiently considered government action in the United States and globally present some of the foremost challenges to the free flow of information online. The State of California, for example, recently passed the California Consumer Privacy Act, which restricts the flow of data, creates significant new compliance costs for companies operating in California and across the country, and puts in jeopardy standard business activities. Among other issues with the law, it creates extremely broad definitions of the terms "personal information" and "sale" that cover vast amounts of innocuous data and activities that may only have been used to support basic business functions. The definition of personal information, for instance, goes beyond definitions in current law to cover virtually any data that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, device, or household including non-personally identifiable information like pixel and cookies IDs.[9] Further, the definition of "sale" includes renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information to another business or third party for monetary or other valuable consideration.[10] These amorphous definitions, and other broadly worded definitions in the law, will run counter to consumers' interests. For instance, the law includes consumer access rights for the specific pieces of personal information a business has collected about a consumer even though the release of this detailed information may lead to consumer fraud, identity theft, or invasions of privacy. The law also includes consumer opt-out rights related to the broad definitions of personal information and sale that could restrict companies from sharing personal information with certain third parties to combat consumer fraud. The law's

[9] Cal. Civ. Code § 1798.140(o).

[10] Cal. Civ. Code § 1798.140(t).

data deletion right, which also rests on broadly worded definitions, creates similar problems that will lead to the deletion of data used to benefit consumers. The effect of the broad and sweeping nature of the data covered by the access, opt-out, and deletion rights will only be fully realized over time, as innocuous data used for legitimate business functions that support the digital economy, including targeted advertising, is haphazardly deleted or blocked from being shared. Compounding these problems, the law creates a private right of action that provides new opportunities to test the limits of these provisions.

The hastily drafted and passed standards in the California Consumer Privacy Act, which supporters of the law already concede need to be amended to provide greater clarity and consistency, are likely to create major compliance costs for businesses large and small and across industry sectors. As a result, the law will impose major costs on the public at large without providing true protection for consumers' privacy interests and sensitive data.

We caution against the issuance of regulation, policies, or legislation such as the California Consumer Privacy Act that could disrupt the digital economy. Patchwork and misguided regulation at the state level that severely burdens the collection and use of data is likely to deter entry, thwart innovation, and limit competition in the sale of online advertising. If online advertising and marketing becomes less effective, it will impede companies' ability to provide online content and services to the public. This could hinder innovation or drive businesses to shift from offering free content and services to demanding direct payment from consumers. This would substantially adversely impact consumers with limited income levels.

Opt-in Models for the Collection, Use, and Sharing of Data. Legislative proposals that include broad opt-in consent requirements regardless of the sensitivity of the data involved are frequently put forward to address alleged privacy concerns, irrespective of any showing of actual consumer harm. These rules would create particular problems for the online ecosystem, impeding consumers' enjoyment of digital-based services while not enhancing consumer privacy.

The imposition of opt-in consent models, where companies cannot collect consumer or device data without consumers first checking a box or taking some other affirmative act, could drastically alter the online experience. Given the collaborative architecture of the internet, data-sharing interactions between website owners and other companies are commonly required for the orderly functioning of a website. These interactions are currently seamless, with little friction to consumers' digital experiences, and are necessary to facilitate website features and online benefits that consumer's value. A requirement for opt-in consent will disrupt this architecture. The constant appearances of consent boxes will annoy and frustrate consumers, and will dilute the impact of such mechanisms.

In the advertising and marketing world, where no record of consumer harm exists to justify a restrictive opt-in standard, we maintain that consumer privacy preferences with respect to advertising and marketing may best be expressed through implied consent or an opt-out standard with exceptions for the use and sharing of data for certain purposes. Opt-in consent has not been the historical standard for advertising and marketing, and is not the appropriate standard for advertising and marketing going forward in any medium. NTIA should carry out systematic analysis of the

GDPR opt-in approach to provide critical data in assessing similar types of efforts that may be offered in the U.S. or elsewhere in the world.

Vague Consumer Data Rights. Legislative proposals related to online privacy often include a variety of consumer rights (*e.g.*, data access and deletion options for consumers) regardless of whether consumer harm is shown. As noted earlier, consumers deserve strong internet privacy protections at a level that ensures that they continue to have access to the full benefits of the internet. The imposition of vague consumer rights with a government imprimatur, such as the consumer rights in the California Consumer Privacy Act and the GDPR, creates a false sense of concern in the public about the use of largely innocuous marketing data as none of these rights are based in demonstrable harms. By extending data access and other rights regardless of marketplace injury, the State of California and the EU are implying that the collection and use of data online generally is harmful, when in fact appropriate data collection brings significant consumer and societal benefits.

Instead of focusing on nonexistent or speculative privacy harms, government action in the United States and globally should focus on supporting privacy protections based on the sensitivity of data, where privacy harms are more likely. The use of data for advertising and marketing allows consumers to receive information about commercial opportunities that they value, and consumers are free to respond (or not) as they see fit. If a consumer does not value a particular message, the consumer will simply ignore it. Moreover, marketing carries societal benefits as a facilitator of economic growth, and is a form of constitutionally protected speech. Against this set of facts, it is unrealistic to suggest that vague rights of access and deletion be extended in a sweeping manner to advertising and marketing databases.

b. Which foreign laws and policies restrict the free flow of information online? What is the impact on U.S. companies and users in general?

The NTIA's notice of inquiry asks for input on the foreign laws and policies that restrict the free flow of information online. The notice of inquiry also asks for input on the impact of these policies on U.S. companies and users in general. As discussed below, in the EU, the newly effective GDPR and the ePrivacy Directive (and the forthcoming ePrivacy Regulation) create onerous requirements that threaten the free flow of information online. Similarly, data localization laws around the world prevent the free flow of information online. Each of these laws impacts U.S. companies as they limit U.S. companies' ability to collect, use, and share data appropriately.

GDPR. The GDPR regulates all aspects of personal data processing, which is intended to include any operation performed on any data point that can be related back to any identifiable (even if unnamed) individual within the EU. Significantly for the advertising and marketing communities, GDPR creates a new opt-in model for consent that is impractical or highly onerous for companies that do not have a direct relationship with consumers.[11] The inability to obtain consent, among other GDPR issues that make it challenging to process EU data, has caused some U.S. companies to stop

[11] GDPR, Article 7.

operating in the EU.[12] Additionally, certain U.S. companies are taking steps to change their services, including discontinuing advertising practices, in order to comply with the new EU laws.

ePrivacy. The ePrivacy Directive of 2002[13] is a companion law to the GDPR that regulates the use of specific technological channels that process personal data, including cookies and online technologies, email, and SMS. The ePrivacy Directive is currently undergoing negotiation as it becomes the ePrivacy Regulation; it is expected that the ePrivacy Regulation will adopt the GDPR's more rigorous consent requirements, which will have detrimental effects on the ability of advertisers, marketers, and data companies to conduct business in the EU. Publishers in Germany, for instance, already are predicting significant losses in revenue; the majority of German magazine publishers recently surveyed predicted that they would suffer losses of more than 30 percent in digital advertising sales due to the ePrivacy rules alone.[14]

***Data Localization*.** In addition to these EU laws, data localization laws around the globe restrict the free flow of information online. Some reports suggest more than two dozen countries now have some form of a data localization law, including laws in China, Russia, Indonesia, and Vietnam.[15] Data localization laws come in a number of forms but at their core these laws require the retention of data within certain jurisdictional borders. Similar to data localization laws, the EU creates restrictions on the export of personal data outside of Europe unless the recipient is in a country deemed to provide adequate privacy protections or if the transferor takes steps to ensure that the transfer of data is protected. Like the data localization laws, the EU's export restrictions create burdens for U.S. companies that seek to operate in the United States and EU as these restrictions limit the collection, use, and sharing of data.[16]

c. What privacy issues should NTIA prioritize?

The NTIA's notice of inquiry asks for input on the privacy issues that NTIA should prioritize. We recommend that that NTIA set as its priority carrying out a rigorous analysis of the GDPR and similar laws to determine their effects on competition and consumers. We also suggest

[12] *See e.g.,* James Hercher, "Drawbridge Exits Media Business In Europe Before GDPR Storms The Castle," Ad Exchanger (Mar. 7, 2018); Ivana Kottasová, "These companies are getting killed by GDPR," CNN (May 11, 2018).

[13] Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

[14] FIPP, "ePrivacy: A loss of more than 30 per cent in digital advertising sales for journalistic media," Insight News (Jan. 31, 2018).

[15] Bret Cohen, Britanie Hall, and Charlie Wood, "Data Localization Laws and their Impact on Privacy, Data Security and the Global Economy," American Bar Association (Fall 2017).

[16] To facilitate the transfer of personal information from the European Union to the United States, both jurisdictions adopted a transfer mechanism called the EU-US Privacy Shield (also, the Swiss adopted an equivalent mechanism with the United States). United States entities that certify to the EU-US Privacy Shield must provide assurances that they will offer privacy protections equivalent to EU law regarding the handling of personal data of European data subjects. If an individual has a concern regarding participants' compliance with the EU-US Privacy Shield, the individual has access to multiple avenues to address their concern, including free dispute resolution, which DMA provides to participating member companies. The DMA serves as a dispute resolution provider under both the EU-US and Swiss-US Privacy Shield frameworks.

that NTIA promote the U.S. sectoral privacy model, offer support for data-driven advertising and marketing, and advocate for industry-self-regulation as part of any privacy regulatory framework.

Analysis of GDPR. We recommend that the NTIA carry out a rigorous analysis on the impacts of GDPR to determine its effects on competition and consumers. We believe the NTIA will find that laws like the GDPR will limit competition, overburden consumers with opt-in notices and make an efficient and effective digital economy harder to maintain. NTIA should share its findings with international bodies and policymakers considering adopting GDPR-like legislation.

Promote the U.S. Sectoral Privacy Model as Opposed to One-Sized-Fits-All Privacy Standards. The U.S. federal privacy model is mainly sectoral and targeted, for instance applying detailed regulations only to specific sectors, industries, practices, or types of data (*e.g.*, financial data, children's data, health data). These sectoral laws are based in the Fair Information Practice Principles, which include notice, choice or consent, access or participation by the individual, data integrity and security, and enforcement or redress. As such, the U.S. privacy model focuses on consumer protection through notice and control, based on potential harms stemming from specific types of data, rather than blanket rules that apply generally across data types and industry sectors. These sectoral laws are supplemented by industry self-regulatory principles to successfully promote the responsible online and offline collection and use of data.

The EU, and other jurisdictions, takes a different approach to privacy regulation, creating comprehensive one-sized-fits-all privacy standards for all sectors of the economy, regardless of data type or potential for harm. The rigid rules of the EU's GDPR, for instance, imposes burdensome opt-in consent requirements and restrictions on data processing that may not be reflective of consumer expectations in each industry. The United States has historically recognized that context matters when regulating privacy. Consumers reasonably expect that companies will use information in ways that are consistent with the context in which consumers provide the data. A one-size-fits-all privacy model is not able to recognize shifting consumer expectations, and therefore will stifle business practices that consumers value and expect.

Support for Data-Driven Advertising and Marketing in the United States and Abroad. The practice of data-driven marketing began in the United States more than a century ago, and the burgeoning data driven marketing economy is a uniquely American creation as well. Just as the United States created digital market-making media by commercializing the internet browser in the 1990s, so it created postal market-making media when Montgomery Ward developed the mail order catalog in 1872. Today, the United States leads the world in data science applied to the marketplace. Ideas developed in the United States by American statisticians and econometricians, running on U.S.-designed hardware, and coded in algorithms developed and tested in the research offices of U.S. firms, are used to generate revenues throughout the world. This has established the data-driven marketing industry as a major export industry and data-driven marketing firms are a net export contributor to U.S. economic well-being. Data-driven marketing firms derive a considerable portion of their revenue abroad (sometimes upwards of 15%) while employing nearly all their workers in the United States.[17]

[17] Deighton and Johnson, *The Value of Data*. See summary of study, at 2, *available at* http://ddminstitute.thedma.org/files/2013/10/DDMI-Summary-Analysis-Value-of-Data-Study.pdf.

Advocate for Industry Self-Regulation in any Privacy Regulatory Framework. The ANA encourages the NTIA to promote industry self-regulation, in addition to the sectoral privacy model that focuses on privacy harms and respects context, as the most effective means to address privacy concerns while promoting innovation. Industry self-regulation is more flexible and adaptable than legislation, and therefore self-regulation can adapt quickly to changes in consumer expectations or available technologies. The ability of a regulatory framework to adapt to changes is especially necessary in the rapidly evolving online and technology marketplaces, where context matters and consumer expectations shift over time. In contrast, legislation tends to be prescriptive and is difficult to update.

The U.S. Congress has considered online privacy issues many times based on ample hearings and debate, and each time has declined to enact legislation providing new generalized authority to the Federal Trade Commission ("FTC"), recognizing that general rules and standards for information practices in this rapidly evolving area would hinder innovation and threaten the economic value of a thriving market sector.[18] In lieu of prescriptive and inflexible government rules, voluntary self-regulatory standards can be used to balance innovation and privacy considerations. Industry bodies, bolstered by the enforcement efforts of federal agencies and state attorneys general, will continue to vigorously enforce self-regulation.

There are a number of industry models for self-regulation of consumer data, including those of the DMA[19] and the Digital Advertising Alliance ("DAA"). The *DMA Guidelines for Ethical Business Practice* ("Guidelines") are one example of longstanding and successful self-regulatory principles that provide meaningful controls and accountability to ensure that marketing data is used responsibly.[20] In October of 2017, DMA announced the release of an updated set of guidelines, including the culmination of its Data Standards 2.0 initiative.[21] The revised standards underscore longstanding responsible data practices that: "Data collected exclusively for Marketing should be used only for Marketing purposes." In fact, the revised standards specifically prohibit the use of data for marketing in the context of eligibility determinations for employment, credit, health care treatment, and insurance, areas of primary concern where actual harm to consumers could occur. Additionally, the standards incorporate data security standards, including provisions related to contractual safeguards, data transfers, and protection of sensitive data.

The Guidelines have been enforced against both DMA members and non-member companies for decades. Such enforcement of the Guidelines has occurred in hundreds of data-driven marketing

[18] The FTC recently came to a similar conclusion in its Internet of Things report, finding that new rules to govern information practices are not needed or appropriate. FTC, *Internet of Things: Privacy & Security in a Connected World* 48-49 (Jan. 2015) (concluding that new privacy rules would be premature and that self-regulation is the appropriate tool to encourage privacy-sensitive practices), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[19] The ANA acquired the DMA on July 1, 2018.

[20] DMA, *Guidelines for Ethical Business Practice* (2017) *available at* https://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/.

[21] Press Release, Data & Mktg. Ass'n,, DMA Announces Final Updated Standards on Marketing Data Use, To Go Into Effect July 2018 (Oct. 10, 2017).

cases concerning deception, unfair business practices, personal information protection, and other practices that could result in injury to consumers. Most companies work to voluntarily cease or change the questioned practices. However, if a company declines to cooperate and a violation of the Guidelines has not been resolved, the matter can be made public and referred to the appropriate regulatory agency.

Another example of successful industry self-regulation related to online privacy is the DAA. Established in in 2009 by the leading advertising and marketing trade associations, the DAA standards address complex policy issues involving the collection and use of web viewing, application use, precise geolocation, and other online data for interest-based advertising and other applicable uses ("Self-Regulatory Program").[22] The DAA Self-Regulatory Program requires companies to inform consumers about their data collection and use practices, and to offer consumers control over DAA covered practices. One of the main avenues through which consumers receive these disclosures and choices is through the DAA's YourAdChoices icon. The icon is served over a trillion times per month worldwide in or around online advertisements delivered through interest-based advertising. The icon provides transparency, and takes consumers to easy-to-use tools to exercise choice for the future collection and use of data for interest-based advertising. Since the launch of the Self-Regulatory Program, participation has grown to encompass hundreds of leading companies and thousands of brands. Over 80 million visitors have now interacted with the DAA's properties. In a study performed in 2016, more than three in five consumers (61%) recognized and understood what the YourAdChoices Icon represents.[23] The program recently was extended to provide greater transparency around political advertising so that voters will receive important disclosures from political advertisers.[24]

Like the DMA's Guidelines, the DAA Self-Regulatory Program shows how industry can respond to the online ecosystem more efficiently than stringent government regulation. If a company fails to meet its obligations under the Self-Regulatory Program, the DAA's independent accountability programs will work to bring a company into compliance and the programs may refer unresolved matters to the FTC. The DAA accountability programs have brought more than 85 enforcement actions since inception, underscoring the responsiveness of the program. The effectiveness of the Self-Regulatory Program also has been recognized by the United States government. In 2012, in an event at the White, the then-Chairman of the FTC, the then-Secretary of Commerce, and Administration officials publicly praised the DAA's cross-industry initiative. The White House recognized the Self-Regulatory Program as "an example of the value of industry

---

[22] DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009); Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data* (Nov. 2011); Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (Jul. 2013); Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015). The NAI Code of Conduct requires similar notice and choice with respect to Interest-Based Advertising.

[23] DAA, *Consumers' recognition of the AdChoices Icon -- and understanding of how it gives choice for ads based on their interests -- continues to rise* (Sep. 29, 2016) https://digitaladvertisingalliance.org/blog/icon-you-see-yeah-you-know-me-0.

[24] DAA, "Digital Advertising Alliance Launches Initiative to Increase Transparency & Accountability in Political Ads," (May 22, 2018), *available at* https://digitaladvertisingalliance.org/blog-terms/political-advertising.

leadership as a critical part of privacy protection going forward."[25] The DAA's work has garnered additional praise, including from former Acting FTC Chairman Ohlhausen who stated that the DAA "is one of the great success stories in the [privacy] space."[26]

Self-regulation, in addition to the U.S. sectoral privacy model that focuses on privacy harms and respects context, has worked for decades to ensure responsible use of data for advertising and marketing purposes, while enabling the growth of a strong data-driven advertising and marketing digital economy. This model stands in clear contrast to GDPR and the California Consumer Privacy Act. We strongly urge the NTIA to undertake a rigorous analysis of the GDPR and similar laws and prioritize policies that create strong consumer internet privacy protections at a level that ensures that consumers continue to have access to the full benefits of the internet and that maintains the United States' leadership in the digital economy.

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the NTIA on these issues. If you have questions, please contact Dan Jaffe at djaffe@ana.net.

Respectfully submitted,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Cc: Stu Ingis, Venable LLP
Michael Signorelli, Venable LLP
Tara Potashnik, Venable LLP
Jared Bomberg, Venable LLP

[25] Speech by Danny Weitzner, We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age (February 23, 2012), *available at* http://www.whitehouse.gov/blog/2012/02/23/we-can-t-waitobama-administration-calls-consumer-privacy-bill-rights-digital-age .

[26] Katy Bachman, *FTC's Ohlhausen Favors Privacy Self-Regulation*, Adweek (June 3, 2013), *available at* http://www.adweek.com/news/technology/ftcs-ohlhausen-favors-privacy-self-regulation-150036.