November 9, 2018

Submitted Via Email: privacyrfc2018@ntia.doc.gov

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

RE: Request for Comment on "Developing the Administration's Approach to Consumer Privacy"

The undersigned trade associations collectively represent thousands of companies, from small businesses to household brands, which engage in responsible data collection and use that benefits consumers and the economy. We provide these comments in response to the National Telecommunications and Information Administration's ("NTIA") request for public comment on "Developing the Administration's Approach to Consumer Privacy" published on September 26, 2018.[1] We and our members believe that the United States' existing privacy framework of targeted sectoral privacy laws, coupled with enforceable self-regulatory programs, and backed by robust enforcement by the Federal Trade Commission ("FTC") is a strong base upon which to build supplemental, consistent, interoperable, national standards to address the developments in the modern data-driven economy. As the data-driven economy continues to provide consumer benefits, drive innovation, and increase economic growth, it is important to calibrate new privacy frameworks to balance the need for competition and responsible marketplace growth with consumers' privacy expectations.

We urge NTIA to continue to advocate for limiting any unreasonable barriers to the responsible collection and use of information in the data-driven economy, such as those imposed by foreign jurisdictions and restrictions emerging in the states. NTIA should promote the adoption of a model that builds on the existing approach of smartly attuned laws focused on concrete consumer harms, supplemented and supported by quickly-adapting self-regulatory programs, to govern the collection and use of consumer data. Local laws that create patchwork standards would break the well-functioning data-driven economy, diminish the value created for consumers, and hurt job creation and innovation.

This goal can be achieved through a preemptive, federal law to set a national standard focused on identifying reasonable data practices, prohibiting unreasonable practices, and using a risk-based approach to prevent concrete consumer harms. This new standard should build on the current system's 20-plus years of success, based on an inherent focus on risk-management, and regulation of data use practices that can cause concrete harm to consumers. Within such a framework businesses can thrive, self-regulatory programs can develop guidelines that outline new reasonable and unreasonable practices to manage the marketplace, and consumers will continue to benefit from innovative digital practices. Such a national standard would bolster the

[1] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 187, 48600-48603 (Sep. 26, 2018) (hereinafter *RFC*).

FTC's already strong enforcement regime, build upon the United States' traditional privacy framework foundation, and avoid the misguided approaches that are giving rise to a patchwork of jurisdiction-specific privacy regimes.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

The free flow of data fuels the economic engine of the data-driven economy. One piston in that engine is data-driven advertising. Data-driven advertising has powered the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising, both offline and on the Internet, supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them.

As a result of this advertising-based model, the data-driven economy in the United States has been able to grow and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem* conducted for the Interactive Advertising Bureau ("IAB") by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.[2] Calculating against those figures, the interactive marketing industry contributed $1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.[3] The study, designed to provide a comprehensive review of the entire Internet economy and answer questions about its size, what comprises it, and the economic and social benefits Americans derive from it, revealed key findings that analyze the economic importance, as well as the social benefits, of the Internet. These benefits require data to be unencumbered by onerous regulations that limit the ability of companies to continue to create innovative new businesses and services.

Consumers, across income levels and geography, embrace the ad-supported model and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to exercise their right to free speech and expression across the globe. They are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store is used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. To the contrary, in a Zogby survey commissioned by the Digital Advertising Alliance ("DAA"), consumers assigned the value of the ad-supported services, like news, weather, video content, and social media they desire and use to be $99.77 per month, or $1,197 a year.[4] A large majority of surveyed consumers, 85%, stated they like the ad-supported model, and 75% indicated that they would

---

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

[3] *Id.*

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

greatly decrease their engagement with the Internet if a different model were to take its place.[5] Indeed, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today.

Responsible data-driven advertising and marketing uses of data are hugely beneficial to consumers individually and to the economy as a whole. As this ecosystem evolved, it did so within a framework of privacy principles that sought to achieve the NTIA's goals for privacy outcomes. As explained in more detail below, and as identified by NTIA, the United States created the "strongest privacy enforcement regime in the world."[6] Consumer transparency, control, data security, and accountability are at the heart of the existing privacy ecosystem. And, these values are the framework upon which the value of the digital economy has increased. Modernizing and adding to the current regulatory system to account for the rise of the digital economy, with national standards for responsible data practices and providing space for self-regulation, is the best way to ensure that the United States continues to benefit from the data-driven economy.

II. Our Industry Provides a Key Example of how the Privacy Framework can Evolve to meet a New Standard

As NTIA notes in its request for comment, the current U.S. legal framework helped the United States take the lead in the data-driven economy.[7] Inherent to this framework is a risk/harm-based management approach that protects consumers from concrete harms. For example, the Health Information Portability and Accountability Act ("HIPAA") regulates certain health data; the Fair Credit Reporting Act ("FCRA") regulates the use of consumer data for eligibility purposes; the Children's Online Privacy Protection Act ("COPPA") addresses personal information collected online from children; and the Gramm–Leach–Bliley Act ("GLBA") focuses on consumers' financial privacy. These risk-based statutes create regulation around areas that could create actual harm for consumers if that data is misappropriated. These risk-based statutes allowed the private sector to develop responsible and reasonable data practices, while prohibiting those practices that could create actual consumer harm. At the core of these laws are the concepts of consumer notice and control, and responsible data practices, all of which lead to the adoption of reasonable data practices in the marketplace.

This framework of sectoral laws is supplemented by industry self-regulatory codes of conduct and the FTC's section 5 authority. This combination has proven to be a successful means of advancing innovation, delivering valuable and relevant content and services to consumers while also protecting consumers through the provision of transparency and control over their data choices. New legislation, regulations, and standards should be layered upon this model, but without jettisoning the existing safeguards and controls for consumers as well as the approach that has fostered innovation by replacing them unduly with burdensome regulatory obligations.

---

[5] *Id.*
[6] *RFC* at 48600.
[7] *Id*. at 48601.

We, our members, and our industry were instrumental in the development of robust industry self-regulation programs that serve as a model for how to identify and address the complex policy issues within the data-driven ecosystem. Both the Digital Advertising Alliance ("DAA") Self-Regulatory Principles, and the Network Advertising Initiative Code of Conduct serve as strong self-regulation for our industry. Our industry worked collaboratively to form the DAA as a self-regulatory program to address intricate policy issues involving the collection, use, and transfer of web viewing and mobile application use data for advertising and other applicable uses. The DAA is unique in self-regulation in the privacy space. It includes an ecosystem-wide scope, independent enforcement, a commitment to regularly updating its guidance in partnership with policy makers, and other notable features. The DAA's Self-Regulatory Program reflects the initial 2009 recommendations by the FTC for self-regulation in the online behavioral advertising space The program has evolved over the last nine years as new technologies and practices emerged in the marketplace to address how those practices can reasonably be used by entities in the ecosystem, such as the rise in the use of mobile apps and cross-device linking.[8] The FTC's original recommendations "supported self-regulation because it provides the necessary flexibility to address evolving online business models," and the DAA's method of assessing and developing reasonable practices for the marketplace takes the lead in this approach.[9] We consider the DAA's focus on providing consumers with meaningful transparency and control over the collection, use, and transfer of data to be the model for how various stakeholders, ranging from the government to industry members, can address data privacy and create flexible, reasonable, solutions.

We also recognize that strong, independent enforcement is the key to any self-regulatory program. Compliance with the DAA Principles is monitored and enforced by two accountability programs—the DMA, a division of the Association of National Advertisers, and the Council of Better Business Bureaus.[10] The Council of Better Business Bureaus' program has brought more than 90 public enforcement actions, and issued several compliance warnings, which dealt with desktop, mobile, native advertising, non-cookie based data collection technologies, cross-device linking, and video advertising.[11] This independent enforcement is further back-stopped by government regulatory agencies such as the FTC. More specifically, if a company fails to come into compliance, the DAA's accountability program will refer that company to the appropriate

---

[8] The term "online behavioral advertising" means the collection of web viewing and application use data from a particular computer or device across non-affiliated Web sites and mobile apps over time in order to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from that web viewing and application use behavior. Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* 10-11 (Jul. 2009) http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (July 2013) http://www.aboutads.info/DAA_Mobile_Guidance.pdf; Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015) http://www.aboutads.info/sites/default/files/DAA_Cross-Device_Guidance-Final.pdf.

[9] Federal Trade Commission, *Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising Tracking Targeting, & Technology*, 11 (Feb. 2009) (hereinafter *FTC Report*) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[10] *See* Council of Better Business Bureaus, *Accountability Program Decisions, Dispositions, Closures, and Guidance* (2018), http://www.asrcreviews.org/accountability-program-decisions/; Data & Marketing Association, *Ethics & Compliance* (2018) https://thedma.org/accountability/ethics-and-compliance/.

[11] *Id.*

regulator.[12] The breadth of the accountability program's actions, and the DAA's willingness to report offenders to government authorities, show the responsive nature and enforceability of the DAA's program and how much further properly constructed self-regulatory models can be extended over time.

A key element of the DAA's program is its restrictions on the use of covered data for certain purposes. Specifically, the DAA prohibits the collection, use, and transfer of web viewing and application use data to determine eligibility for employment, credit, health care treatment, or insurance eligibility and underwriting.[13] We worked with our members and industry as a whole to identify potentially harmful, unreasonable, practices and ban them from the marketplace. While those harmful and unreasonable practices were never part of the industry's customs, the industry collectively decided to prevent them from ever coming into practice. Similar systems and practices could be layered on and support a preemptive national standard across the various parts of the Internet that is implemented to build upon the current framework.

The successful approach taken by the DAA led to a February 2012 event at the White House where the then-Chairman of the FTC, the then-Secretary of Commerce, and other Administration officials publicly praised the DAA. The White House recognized the DAA as "an example of the value of industry leadership as a critical part of privacy protection going forward."[14] The DAA also garnered kudos from then-Acting FTC Chairman Maureen Ohlhausen who stated that the DAA "is one of the great success stories in the [privacy] space."[15] In its cross-device tracking report, the FTC staff also stated, "...DAA [has] taken steps to keep up with evolving technologies and provide important guidance to [its] members and the public. [Its] work has improved the level of consumer protection in the marketplace."[16]

Using this model as scaffolding to build upon and expand, the NTIA can ensure that a broad risk-based approach combines national legislation and self-regulatory programs to identify and regulate reasonable and unreasonable data practices as a way to respond to the ever changing nature of the data-driven economy. This new system will create legal and regulatory standards that enhance the existing framework, keeping the privacy framework in the United States in step with the evolving marketplace, and preventing the exploitation of unreasonable data practices that could lead to consumer harm.

---

[12] In its history, the accountability program has only needed to refer one company for none compliance. *See* ASRC, *SunTrust Bank Referred to the CFPB for Refusal to Participate in Self-Regulation* (May 8, 2014) http://www.asrcreviews.org/suntrust-bank-referred-to-the-cfpb-for-refusal-to-participate-in-self-regulation/.

[13] Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment*, 31-32 (2013).

[14] 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.

[15] 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.

[16] Federal Trade Commission, *Cross-Device Tracking: An FTC Staff Report*, 10 (Jan. 2017).

III. Newly Developed Privacy Regimes, both in the United States and Abroad, Harm this Well-Functioning Ecosystem and the Administration Should not Follow Suit

Even though the existing framework has enabled unprecedented growth and consumer benefit, some actors (both in the United States and abroad) seek to break that system with restrictive and irresponsible legislation. NTIA should take lessons learned from recent developments as it seeks to build upon the current U.S. system. Jurisdiction specific regulation, such as the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"), threaten to balkanize the Internet within walled gardens that will sap economic growth, confuse consumers, harm competition by locking out startup and small business opportunities, and ultimately fail to provide the very privacy "protections" they purport to deliver. Therefore, NTIA should work to improve upon the 20-plus years of successful privacy regulation in the United States in conjunction with the stakeholders that intimately understand that ecosystem.

Evidence of the unintended consequences from these restrictive policies is demonstrated by the harm that the GDPR has already caused to the European marketplace. Prior to the GDPR's enforcement date, many U.S.-based companies left the European market instead of facing crippling regulations and potential fines. For example, according to media reports some United States based advertising companies, consulting services, and video game developers decided to exit the market, forego potential revenue, and no longer employ their European employees instead of risk violation of the restrictive requirements of the GDPR.[17] In addition to firms exiting the European marketplace, at least one major United States newspaper elected to charge its European subscribers a $30 premium to access its content to compensate for the fact that it is unable to effectively advertise to those consumers due to the GDPR.[18]

Parts of the misguided approach taken by the European Union are now being imported to the United States in the form of the CCPA. The CCPA is not a mirror image of the GDPR, which means companies will need to comply with competing regulatory requirements based on the jurisdictions they operate in. Beginning on January 1, 2020, businesses will be required to treat their customers from California in a materially different manner than other American customers. California consumers will be inundated with new notifications and requests from the services they seek. Instead of offering any material enhancements to consumer privacy, the CCPA will likely result in consumer confusion, frustration, and a severe case of buyer's remorse.

This rising cost of regulation is removing consumer choice for content and services from the European marketplace without providing countervailing consumer benefits, and it is limiting competition that is the lifeblood of the Internet marketplace. California elected to rush to follow that model, resulting in poorly crafted legislation that fails to provide consumers with any benefits to counteract the harm the CCPA will cause. These approaches stand in stark contrast to the history of the United States privacy framework, where our well-reasoned sectoral laws and

---

[17] Hannah Kuchler, *Financial Times, US small businesses drop EU customers over new data rule* (May 24, 2018) https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

[18] Lucia Moses, *Digiday, The Washington Post puts a price on data privacy in its GDPR response — and tests requirements* (May 30, 2018) https://digiday.com/media/washington-post-puts-price-data-privacy-gdpr-response-tests-requirements/.

strong enforcement regimes, coupled with industry self-regulation that identifies, promotes responsible uses of data, and holds companies accountable. This approach created the flourishing U.S.-based data-driven economy.

NTIA and other members of the administration can use California's mistake to its own advantage. This is an opportunity to research how negatively the CCPA's approach will impact consumers and the economy. As NTIA noted in its request, the United States should continue to promote a cohesive, interoperable, harmonious approach to privacy. An increasingly fragmented patchwork of laws at the state, local, and international level should be rejected in favor of legal standards that set a standard applicable to all businesses and consumers alike.

In many ways, the United States' risk-based sectorial framework discussed above remains the most robust and effective privacy framework in the world. The NTIA should not rush to judgement and follow the misguided lead of Europe and California. The Administration should instead continue to work with industry and a broad swath of stakeholders to evolve the 20-plus year old privacy framework this country developed. The administration should build upon the United States' time-tested approach, based in smartly drafted legislation and regulations, to create a new cohesive national standard that identifies reasonable and unreasonable practices supplemented by self-regulatory programs (backed by independent enforcement programs). The FTC is well-suited to continue as the lead enforcer in this area, leveraging its authority under Section 5 of the FTC Act. Such an approach will ensure that the United States continues to lead the Internet economy for decades to come.

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the NTIA on this issue. If you have questions, please contact Michael Signorelli at 202.344.8050.

Respectfully submitted,

American Advertising Federation
American Association of Advertising Agencies
Association of National Advertisers
Interactive Advertising Bureau
Network Advertising Initiative

November 9, 2018

CC: Stu Ingis, Venable LLP
Rob Hartwell, Venable LLP