Before the
National Telecommunications and Information Administration
Washington, DC 20230

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on

Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780–8780–01

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street, NW
Suite 660
Washington, DC, 20006
202.296.1883

Counsel:
Stu Ingis
Tara Potashnik
Jared Bomberg
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

November 6, 2018

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 comment on "Developing the Administration's Approach to Consumer Privacy" published on September 26, 2018 ("RFC").[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 solutions 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 RFC provides guideposts for future privacy regulations in the United States, including the RFC's focus on a risk-based framework and a need to account for context when determining privacy expectations. Some jurisdictions, such as the European Union ("EU") and California, recently have taken a more restrictive approach to regulating data, choosing to treat all data the same regardless of the risk or context. This overly restrictive approach threatens the free flow of information that is vital to delivering the products and services that consumers value and expect. We urge the NTIA to prioritize advocacy for consumer privacy protections that will create a single, national standard calibrated to ensure that consumers continue to have access to the full benefits of the Internet and that maintains the United States' leadership in the digital economy. To this end, ANA supports considering new solutions to address privacy considerations, and we address some of these ideas further in Sections III and IV of these comments.

I. The U.S. Regulatory Approach to Data Has Helped Foster a Data-Driven Economy that Is the Envy of the World

The data-driven economy has grown rapidly in the United States due in part to a carefully crafted regulatory system that encouraged innovation. In its 1997 "Framework for Global Electronic Commerce," the Clinton administration stated that "[t]he private sector should lead [and] [t]he Internet should develop as a market driven arena not a regulated industry."[2] The Clinton administration also argued that "governments should encourage industry self-regulation and private sector leadership where possible" and "avoid undue restrictions on electronic

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

[2] The White House, The Framework for Global Electronic Commerce: Executive Summary (1997).

commerce."[3] At the time, the government considered comprehensively regulating the Internet and related connectivity through formal legislation, and ultimately adopted the approach we have today, which is a "sectoral" framework that addresses particular areas of concern such as children's online privacy or specific sectors perceived as handling sensitive information (*e.g.*, healthcare and financial services). These sectoral laws are complemented by industry self-regulatory principles to successfully promote the responsible online and offline collection and use of data.

Looking back over the last 20 years of the growth of the Internet and the data-driven economy, former Acting Chairman of the Federal Trade Commission ("FTC"), Maureen Ohlhausen said, "The success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors."[4] Echoing this sentiment, FTC Chairman Joe Simons recently cautioned that, "if you do privacy in the wrong way, have it go too far in one direction…you might end up reducing competition."[5]

It is our agile, flexible and consistent framework of protections that has created a platform for innovation and tremendous growth opportunities for U.S. companies. The ability of consumers to provide, and of companies to responsibly collect and use, consumer data has been an integral part of this framework. Every day, consumers' lives are enriched by data-driven resources and advertising, including an unprecedented array of high-quality information, entertainment, and life-enhancing services. Revenues from online advertising based on the responsible use of data 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.[6] The collection and use of data is now integral to our daily lives and to U.S. economic competitiveness. A study led by Prof. John Deighton at the Harvard Business School reported that the ad-supported Internet ecosystem

[3] *Id.*

[4] Maureen K. Ohlhausen, Comm'r, Address at the FTC Internet of Things Workshop: The Internet of Things: When Things Talk Among Themselves 1 (Nov. 19, 2013).

[5] *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy and Commerce*, 115th Cong. (2018).

[6] In a recent Zogby survey, 90% of consumers stated that free content was important to the overall value of the Internet and 85% surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content. Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016). The Zogby survey also found that consumers value the ad-supported content and services at almost $1,200 a year. 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).

generated $1.121 trillion for the U.S. economy and was responsible for 10.4 million jobs in the United States in 2016.[7]

The NTIA has already shown through this RFC that it recognizes the value of data and its importance to innovation, stating in the very first sentence of the RFC that the NTIA "is requesting comments on ways to advance consumer privacy *while protecting prosperity and innovation*."[8] The RFC further states, "Every day, individuals interact with an array of products and services, many of which have become integral to their daily lives. Often, especially in the digital environment, these products and services depend on the collection, retention, and use of personal data about their users."[9] Accordingly, to promote the values the NTIA articulated in the RFC and to support U.S. innovation, competitiveness, and consumer benefits, any NTIA action on privacy should serve to protect the ability of brands and marketing solutions providers to collect and use data responsibly and continue the time-tested policy of avoiding "undue restrictions on electronic commerce" that has served U.S. consumers and businesses so well for the last twenty years.

II. The NTIA's RFC Presciently Highlights the Problem of an Emerging Fragmented Regulatory Landscape; the U.S. Data-Driven Economy and Consumer Interests Are Now Under Unwarranted Threat by New, Ill-Conceived, State-Based and International Privacy Laws that Are Splintering the Regulatory Structure

The NTIA's RFC notes that, "A growing number of foreign countries, and some U.S. states, have articulated distinct visions for how to address privacy concerns, leading to a nationally and globally fragmented regulatory landscape. Such fragmentation naturally disincentivizes innovation by increasing the regulatory costs for products that require scale."[10] To that point, stakeholders across the marketplace are raising alarms with respect to the defective provisions of the new California Consumer Privacy Act ("CCPA") and the newly operative European Union General Data Protection Regulation ("GDPR"),[11] which will have potentially damaging implications for U.S. businesses and consumers.[12]

---

[7] John Deighton, Leora Kornfeld, Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, IAB (2017); John Deighton & Peter Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy*, the DMA (2015); John Deighton & Peter Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy*, the DMA (2013).

[8] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 187, 48600 (Sept. 26, 2018) (emphasis added).

[9] *Id.*

[10] *Id.*

[11] Cal. Civ. Code § 1798.100; 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.

[12] Dan Jaffe, *Fixing the California Privacy Law Will Require a Serious, Long Term Effort*, ANA (Sept. 4, 2018); Sarah Boot, *No Time to Waste on Fixing Consumer Privacy Law*, CalChamber (Aug. 20, 2018).

Among the many serious problems created by the CCPA is its extremely broad definition of the term "personal information," which includes vast amounts of innocuous data and activities. The definition covers, for example, 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.[13] Given that this definition could cover nearly any type of data, including someone's pizza topping choice or the type of operating system used in a mobile device, California has created a law that regulates data well beyond addressing privacy concerns. As a result, the CCPA's rules greatly restrict all data used for consumers' benefit even when no privacy risk is associated with the data.

Compounding these problems, the law will cover many small businesses and businesses that have very limited interactions with California consumers. For instance, any company that does business in California and obtains the personal information of 50,000 or more consumers, households, or devices is covered. This means that an online retailer that has 137 devices in California frequent its website each day (out of a population of approximately 40,000,000 Californians) would be covered. Also, according to the CCPA, any business that has annual *gross* revenues in excess of $25,000,000 and collects consumers' personal information would be covered. The CCPA, thus, covers businesses that have gross revenues that meet the threshold but that may be unprofitable and out-of-state businesses that meet the gross revenue threshold but that may only have data from a single California consumer that purchases a product online. These overly broad definitions will result in onerous obligations on small businesses and businesses that have little interaction with California consumers.

The CCPA also includes a number of provisions that run directly counter to consumers' interests. For instance, the law includes consumer access rights (including the rights of third parties to access data) for the specific pieces of personal information a business has collected about a consumer even though the breach or inappropriate release of this detailed information may lead to consumer fraud, identity theft, or invasions of privacy. To this point, former Chairman of the FTC Deborah Majoras stated that "requiring data merchants to provide consumers access to sensitive information may itself present a significant security issue – in some cases, it may be difficult for the data merchant to verify the identity of someone who claims to be a particular consumer demanding to see his or her file."[14] Creating further problems for consumers, the CCPA includes consumer opt-out rights that could restrict companies from sharing personal information with certain third parties to combat consumer fraud. Finally, and potentially most dangerously, the CCPA creates a private right of action based on claims of inadequate data security with statutory damages that are uncapped in the aggregate. The CCPA allows for damages to be recovered up to $750 per consumer per security incident or actual

[13] Cal. Civ. Code § 1798.140(o) (emphasis added).

[14] Letter from FTC Chairman Majoras to Senator Bill Nelson (Jun. 14, 2005).

damages, whichever is greater.[15] This level of penalty could lead to hundreds of millions of dollars in penalties for a data breach even in instances where a security incident has not resulted in consumer harm. These are simply a few of the many ways in which the CCPA threatens to harm consumers and businesses; the effect of the broad and sweeping nature of the CCPA will only be fully realized over time.

Similar problems have emerged with the GDPR, which imposes hundreds of rules on the collection and use of data regardless of the sensitivity of the data or the context of the consumer interaction. In particular, the GDPR imposes burdensome opt-in consent requirements to use consumer data and restrictions on data processing that may not reflect consumer expectations or choice. As a result, all but the largest companies with direct consumer relationships may be cut off from data they need to provide the products and services consumers value and expect. The GPDR has been in effect for less than six months, but it is already clear that it is freezing out competition and hindering smaller companies in the marketplace that may not be able to obtain consumer consent, even though consumers rely on their services. Many U.S. firms have already left the European marketplace as a result of this law, taking choices away from EU consumers and depriving them of the benefits of competition in an open and free marketplace.[16] Additionally, by imposing costly new compliance programs, the GDPR creates significant, and possibly insurmountable, barriers for small and medium sized businesses seeking to compete with large firms that are able to absorb those costs. This will lead to a few winners, and many losers, in the marketplace, picked in part by government regulations.

In the United States, many brands and marketing solutions providers soon will have to comply with both the GDPR and the CCPA, which means they will be left to figure out how to best meet the terms of overlapping and inconsistent rules that create costly compliance challenges and confusion for consumers. These new rules, and potential additional variations on these rules passed by other states, are creating a balkanized patchwork of regulations that consumers will not understand and that serve as a major barrier to entry. The NTIA should work to avoid such a situation in the United States, and work with stakeholders to prevent additional CCPA or GDPR-like regulations from harming U.S. consumers and businesses.

III. A New Privacy Paradigm Is the Best Way to Achieve the Privacy Outcomes and Values Articulated by the NTIA in the RFC

The NTIA's RFC specifically requests public comment on "a set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy."[17] As further described below, the NTIA's "privacy outcomes" can

[15] Cal. Civ. Code § 1798.150.

[16] Hannah Kuchler, *Financial Times, US small businesses drop EU customers over new data rule* (May 24, 2018).

[17] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 187, 48600 (Sept. 26, 2018).

best be achieved through a new privacy paradigm ("New Paradigm") to be enforced by the FTC as a single national standard.

The New Paradigm, as we envision it, provides a new way for businesses, consumers, and regulators to determine when a data collection or use practice is reasonable under the law. The New Paradigm could create a stand-alone privacy standard in the FTC Act that prohibits unreasonable data collection and use practices and provide clarity to businesses by defining *per se* "reasonable" and *per se* "unreasonable" data practices. All *per se* unreasonable data collection or use acts or practices would be new violations of the FTC Act while *per se* reasonable data practices are permissible since they would create little to no risk of consumer harm. These categories would, in effect, create a structural approach to resolving subjective questions of user privacy. Below are examples of potential *per se* reasonable and *per se* unreasonable data practices as well as a mechanism to determine the reasonableness of future uses of data.

- **Per Se Reasonable Practices.** *Per se* reasonable practices, for example, could include the collection and use of non-sensitive data for advertising purposes with consumer transparency and choice. Such advertising practices benefit consumers, are non-harmful, and enjoy longstanding First Amendment protections. By providing consumers transparency and choice, consumers will be in a position to decide whether they wish to receive the benefits of interest-based advertising from certain companies and they have the ability to change their preferences over time. Another set of *per se* reasonable practices includes data activities in compliance with an existing commercial law regulating consumer data. For instance, compliance with existing commercial privacy laws such as the Gramm-Leach-Bliley Act of 1999, the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act of 1970, the Fair Debt Collection Practices Act, the Family Educational Rights and Privacy Act of 1974, the Children's Online Privacy Protection Act of 1998, and the Electronic Communications Privacy Act of 1986 (commercial portions only) would be deemed *per se* reasonable. The RFC states that the NTIA does not propose changing current sectoral laws; similarly, the New Paradigm does not set out to replace these laws; which we would argue should include the above list.

- **Per Se Unreasonable Practices.** *Per se* unreasonable practices, for instance, could include certain data collection and use practices that discriminate based on: employment eligibility, credit eligibility, health care treatment eligibility; insurance eligibility, underwriting, and pricing; education and financial aid eligibility; and housing eligibility.

- **All Other Data Practices Are Designated Through a Defined Process.** Data collection and use practices that are not initially classified in the *per se* reasonable or *per se* unreasonable categories will be designated as reasonable or unreasonable based on set criteria under the New Paradigm. For instance, either through an enforcement action or rulemaking, data collection and use practices will be reviewed for reasonability using

criteria such as the following: (1) the benefits or harms to consumers; (2) consumer expectations; (3) privacy by design controls; and (4) impacts on innovation.

The NTIA requests comments on a number of particular privacy "outcomes" that are captured by the New Paradigm's standard for reasonableness. In particular, the NTIA asks for comments on "transparency" and "control," noting that users should be able to understand how an organization handles their personal information and should be able to exercise reasonable control over the collection, use, storage, and disclosure of their personal information. The New Paradigm captures both "transparency" and "control" in its test for reasonableness, since a factor in the test would likely be whether the data practice meets consumer expectations. If an organization provides consumers clear disclosures and choice regarding the collection and use of the consumer personal information, such practices would weigh in favor of determining that a consumer's expectations are being met and that the practice is reasonable. Conversely, if inadequate disclosures are made and no choice or control is provided, such practices, depending on the circumstance, would weigh in favor of determining that consumer expectations are not being met and the practice is unreasonable.

A benefit of the New Paradigm is that each of the NTIA's "outcomes," as well as others that may develop over time, can be addressed in a flexible manner. The New Paradigm does not require that each of the "outcomes" must always be present but instead weighs these outcomes based on the sensitivity of data, the benefits to consumers and their expectations, the potential impact on innovation, as well as other factors relevant to the inquiry. In this sense, the New Paradigm meets the NTIA's goal of creating "risk-based flexibility." Under the New Paradigm, practices that are deemed *per se* unreasonable would be unlawful even if the company engaging in those practices complied with the "outcomes" presented in the RFC.

The New Paradigm has the potential to clarify data practices for consumers and businesses and provide the protections and flexibility needed to ensure the data-driven economy can continue to grow. Instead of a one-size-fits-all model as has been proposed by the CCPA and the GDPR, the New Paradigm recognizes that consumers benefit from privacy protections that are based on risk and reflect their expectations.

IV. A New Privacy Paradigm Provides a Roadmap for High-Level Privacy Goals for the NTIA

The NTIA requests public comment on "a set of high-level goals that describe the outlines of the ecosystem that should be created."[18] To this end, the New Paradigm provides a set of goals for the NTIA to work towards, the foremost of which is advocacy for the passage of federal legislation that creates a single national standard and that can can create a reasoned framework for efforts to push back against the aspects of the GDPR's and CCPA that put forward misguided approaches to protecting consumer privacy.

[18] *Id.*

The NTIA's RFC notes that the "time is ripe for this Administration to provide the leadership needed to remain at the forefront of enabling innovation with strong privacy protections" and that a "nationally and globally fragmented regulatory landscape" disincentives innovation.[19] To reduce fragmentation nationally and to move toward a globally interoperable framework, we urge the NTIA to advocate for a new national standard for privacy regulation, such as the New Paradigm.

Additionally, to fully understand the scope of the impact of the CCPA and the GDPR, and to inform future policy decisions, the NTIA should carry out a detailed review of the effects of the CCPA and the GDPR on competition and consumers. We anticipate that the NTIA will find that laws like the GDPR and the CCPA will limit competition, overburden consumers with opt-in notices, and make an efficient and effective digital economy harder to maintain. The NTIA should share its findings with policymakers considering GDPR or CCPA-like legislation. Such research will be critical to the formulation of well-informed policy decisions and enforcement priorities.

* * *

The ANA appreciates this opportunity to comment on the appropriate privacy framework for promoting both consumer protection and innovation. Please contact Dan Jaffe, Group Executive Vice President, at djaffe@ana.net or (202) 296-2359 with any questions regarding this comment. We look forward to continuing to work with the NTIA on these issues.

[19] *Id.*