Before the
Federal Trade Commission
Washington, DC 20024

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on the

FTC Hearing on Competition and Consumer Protection in the 21st Century – February 2019

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

December 17, 2018

On behalf of the Association of National Advertisers ("ANA"), we provide comments in response to the Federal Trade Commission's ("FTC" or "Commission") request for public comment on the "FTC Hearing on Competition and Consumer Protection in the 21st Century – February 2019," ("Hearing") which will focus on consumer privacy.[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 FTC's Hearing announcement asks a series of questions about matters of consumer privacy, including inquiries on the benefits to consumers from the collection, sharing, and use of consumer-related data, as well as the efficacy of various privacy legal frameworks. In these comments we provide: (1) an overview of the historic U.S. regulatory approach to consumer-related data and the benefits of this approach; (2) the risks associated with new data restrictions passed in Europe and California and that other U.S. states are considering; and (3) recommendations for consumer privacy protections that will ensure that consumers continue to have access to the full benefits of data and that maintain the United States' leadership in the digital economy. Given the changing privacy regulatory approach in the states, with states seeking to regulate data in the consumer context each in their own unique way, and the risk of complete fragmentation of the U.S. privacy landscape to the detriment of consumers and businesses alike, we urge the FTC to advocate for the passage of federal legislation, preemptive of state laws, that creates a single national standard such as the New Paradigm model we discuss in section III of these comments, without also replacing all existing federal consumer privacy laws. We also recommend that the Commission carry out a rigorous analysis on the impacts of alternative privacy frameworks, such as the EU's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act of 2018 ("CCPA"), to determine their effects on competition and consumers.[2]

[1] FTC, *FTC Hearing on Competition and Consumer Protection in the 21st Century - February 2019*, available at: https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019.

[2] Cal. Civ. Code § 1798.100 (effective Jan. 1, 2020); 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).

I. The U.S. Regulatory Approach to Data Has Fostered 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 encourages 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."[3] The Clinton administration also argued that "governments should encourage industry self-regulation and private sector leadership where possible" and "avoid undue restrictions on electronic commerce."[4] At the time, the government considered comprehensively regulating the Internet and related connectivity and data 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, a former Acting Chairman of the FTC 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."[5] 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."[6]

Our agile, flexible and consistent framework of protections creates 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, data about consumers 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.[7] The collection and use of data is now

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

[4] *Id.*

[5] 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).

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

[7] In a 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-*

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 generated $1.121 trillion for the U.S. economy and was responsible for 10.4 million jobs in the United States in 2016.[8]

The FTC recognized in its Hearing announcement that data and data-driven technologies can provide benefits to consumers, stating that, "Consumers have benefited from the proliferation of mobile apps, mobile payment systems, Internet-connected devices (i.e., the Internet of Things), and other innovations."[9] The FTC asked in its Hearing announcement for the public to describe the "actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use."[10] The FTC's emphasis on the benefits of data and data-driven technologies is consistent with the Commission's longstanding view of the importance of data in the digital economy.[11] Accordingly, to further reap the benefits of data, the FTC has long supported policies to promote U.S. innovation, competitiveness, and consumer privacy. Any FTC action on privacy should serve to protect the ability of brands and marketing solutions providers to collect and use data responsibly and continue the United States' time-tested policy of avoiding "undue restrictions on electronic commerce" that has served consumers and businesses so well for the last twenty years.

II. 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 FTC's Hearing announcement notes that, "Some jurisdictions have enacted new laws that contain new approaches for addressing privacy risks," such as the EU GDPR and U.S. state laws.[12] Such fragmentation places a burden on consumers who must manage their own privacy based on multiple and inconsistent legal frameworks and hurts businesses that must set up unique processes to comply with the various laws. To that point, stakeholders across the marketplace are raising alarms particularly with respect to the defective provisions of the new CCPA and the

Supported Online Services Worth $1,200/Year; 85% Prefer Ad-Supported Internet to Paid, PR Newswire (May 11, 2016).

[8] 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).

[9] FTC, *supra* note 1.

[10] *Id.*

[11] FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, 2 (Mar. 2012) ("the collection and use of consumer data has led to significant benefits in the form of new products and services.").

[12] FTC, *supra* note 1.

newly operative GDPR, which will have damaging implications for U.S. businesses and consumers.[13]

Among the many issues created by the CCPA is its extremely broad definition of the term "personal information" within the law's privacy-related provisions, 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.[14] 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, the CCPA covers any company that does business in California and obtains the personal information of 50,000 or more consumers, households, or devices. 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 is 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 purchasing one of their products online. These overly broad definitions will result in onerous obligations on small and struggling businesses and businesses that have little interaction with California consumers. The CCPA becomes operative on January 1, 2020. Due to the law's 12-month look-back provision,[15] businesses may need to start retaining data as early as January 1, 2019, which provides very little time for entities to update databases and systems for compliance purposes and to meet consumer expectations. These technology changes will be especially challenging because the CCPA rulemaking has not yet begun; without this guidance, businesses do not have clarity on, for instance, the systems that need to be built or the specific data that will be covered.

The CCPA also includes a number of provisions that run directly counter to consumers' interests. For instance, the law includes third party access rights 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, a former Chairman of the FTC stated that, "requiring data merchants to provide consumers access to sensitive information may itself present a significant

[13] 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); Forbes Technology Council, *15 Unexpected Consequences of GDPR*, Forbes (Aug. 15, 2018).

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

[15] *See e.g.* Cal. Civ. Code § 1798.130(a) ("The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request").

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."[16] 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. Also, the CCPA creates limitations on individualized pricing and benefits that threatens the continued use of loyalty programs and similar discounts that companies traditionally provide and that consumers value.[17] Additionally, 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 damages, whichever is greater.[18] 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 issues 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 data about consumers and restrictions on data processing that may not reflect consumer expectations or choice. As a result, consumers are inundated with click-through privacy notices and 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 just over six months, but it is already clear that it is freezing out competition, hurting consumers, and hindering companies in the marketplace. For instance, across the non-advertising ecosystem, a number of businesses chose to exit the European market to avoid compliance costs and potential fines, and since the GDPR has been in effect there has been an estimated decrease in startup investment of 40-percent.[19] Consumers' ability to access online content also has been significantly impacted, with more than 1,000 United States based publishers blocking access to their content in part because of the inability to profitably run advertising.[20] Following the GDPR's May 2018 enforcement date, the volume of programmatic advertising in Europe reportedly dropped between 25 and 40 percent across exchanges.[21] 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,

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

[17] Cal. Civ. Code § 1798.125.

[18] Cal. Civ. Code § 1798.150.

[19] Ivana Kottasová, *These companies are getting killed by GDPR* (May 11, 2018); Mark Scott *et al*., *Six months in, Europe's privacy revolution favors Google, Facebook,* CNNBusiness (Nov. 23, 2018).

[20] Jeff South, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect*, Nieman Lab (Aug 7, 2018).

[21] Jessica Davies, *GDPR mayhem: Programmatic ad buying plummets in Europe*, DigiDay *(*May 25, 2018).

including hurting consumers who have lost access to many products and services they value, in a 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 FTC should work to avoid such a situation in the United States, and work with policymakers to discourage 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 Long-Espoused by the FTC

The FTC's Hearing announcement states that "now is the right time for the Commission to re-examine [its] approach" to consumer privacy.[22] To reduce fragmentation across the United States, ensure the FTC's continued position as the lead regulator of consumer privacy, and to maintain U.S. leadership in the digital economy, we urge the FTC to advocate for a new national standard (such as the New Paradigm) for privacy regulation without also replacing all existing federal consumer privacy laws.

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 would empower the FTC to prohibit 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 would be 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 able to decide whether they wish to receive the benefits of interest-based advertising from certain companies and also change their preferences over time. Another set of *per se* reasonable practices includes data activities permitted by existing commercial law regulating consumer-related data. For instance, activities permitted by commercial privacy laws such as the Gramm-Leach-Bliley Act of 1999, the Health Insurance Portability and Accountability Act of 1996, the Fair Credit

[22] FTC, *supra* note 1.

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.

- ***Per Se* Unreasonable Practices.** *Per se* unreasonable practices, for instance, could include determining adverse terms or conditions or ineligibility for an individual's: employment; credit; health care treatment; insurance; education and financial aid; and housing. Additionally, *per se* unreasonable practices could include: the collection, use, and sharing of certain sensitive data without consent; fraudulent behavior that leads to privacy violations; and the use of a person's race, religion, or sexual orientation to set the price for a product or service.

- **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; and (3) relevant risk management practices of the business with respect to the data practice in question.

The FTC's Hearing announcement requests comments on a number of privacy practices that are captured by the New Paradigm's standard for reasonableness. In particular, the FTC asks for comments on consumer notice and choice, including whether "consumers [can] be provided the right balance of information, i.e., enough to inform the choice, but not so much that it overwhelms the decisionmaker?" The New Paradigm captures both notice and choice in a number of ways, including in its main 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 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.

The New Paradigm has the potential to clarify data practices in a manner that will promote business compliance and improve privacy protections for consumers. The New Paradigm also provides the 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 FTC

The FTC requests public comment on "whether other approaches [to address consumer privacy] might better serve consumers and competition; and, if so, what those approaches should be." To this end, the New Paradigm provides a new approach for the FTC to work towards, the foremost of which is further use of a reasonableness standard. The benefits or harms to consumers, consumer expectations, and relevant risk management practices of the involved business with respect to the data practice in question can be further integrated into the Commission's authority and guidance materials.

Additionally, the FTC's status as the nation's lead regulator of consumer privacy should continue and the FTC should advocate for a national legal framework, preemptive of state laws, to ensure that outcome. Given the changing privacy approach in the states, and the risk of complete fragmentation of the U.S. privacy landscape to the detriment of consumers and businesses alike, we urge the FTC to advocate for the passage of federal legislation that creates a single national standard enforced by the FTC, without also replacing all existing federal consumer privacy laws, that is based on a reasoned framework such as the New Paradigm.

Finally, to fully understand the scope of the impact of the CCPA and the GDPR, and to inform future policy decisions, the FTC should carry out a detailed review of the effects of the CCPA and the GDPR on competition and consumers. We anticipate that the FTC 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 FTC 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 FTC on these issues.