November 9, 2018

Submitted Via Email: privacyrfc2018@ntia.doc.gov

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

Re: UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS INFORMATION ADMINISTRATION
REQUEST FOR PUBLIC COMMENT:
DEVELOPING THE ADMINISTRATION'S APPROACH TO CONSUMER PRIVACY
DOCKET NO. 180821780-8780-01

On behalf of the membership of MPA - The Association of Magazine Media (MPA), we are pleased to submit the following response to the National Telecommunications Information Administration's (NTIA) recent request for public comment for "Developing the Administration's Approach to Consumer Privacy" (Docket No. 180821780-8780-01) (September 26, 2018). As the national trade association for the consumer magazine industry, MPA represents approximately100 domestic magazine media companies with more than 900 national publications that span an enormous range of genres across print and digital media. Our members connect more than 90 percent of all U.S. adults to the print and digital magazine titles they trust and value most.

MPA and our members believe there is a need for federal action on privacy. In 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have general or specific laws imposing varying levels of data privacy, security, and breach notification requirements on entities holding consumer data. As the NTIA noted in its request for public comment, this patchwork of competing and inconsistent baseline laws "harms the American economy and fails to improve privacy outcomes for individuals". MPA agrees with NTIA's assessment. Following the recent passage of the *California Consumer Protection Act*, which creates a vast array of restrictions on the handling of data, the need for a uniform, risk-based federal standard has never been more important.

In addition to these comments, we also endorse the attached comments being filed with NTIA today by a coalition of data-driven associations across industries. These comments encourage NTIA to consider and support a new privacy regulatory paradigm that can serve as a guide to regulators, consumers, and market participants to distinguish between reasonable and unreasonable data practices. The associations also encourage the Administration to take action to address the emerging fragmentation in state privacy laws and to analyze and report on the impact of proposed privacy frameworks and emerging state laws on consumers and the economy.

I. A Reasonableness Standard Supports the First-Party, Customer-Facing Relationship Between Publishers and Consumers

Magazine publishers have a consumer-facing, first-party relationship with their customers, and are a trusted source for information and entertainment. Our industry's approach to privacy is built on consumer expectations and trust. It is designed to foster an environment of confidence that strengthens the bond between publisher and reader. Whether consumers subscribe to magazines or consume our content by visiting our websites and digital platforms, consumers take an active role in interacting with our brands. Magazine customers give publishers their personal information because they have a reasonable expectation for how the information will be used and are given choices to limit sharing of their information.

Because of our first-party relationship with long-term customers, our transparency and choice procedures and options are well-established and well-known. Publishers provide multiple, widely-available touch-point options for consumer interactions, including physical addresses, telephone numbers, web sites, and/or email addresses. For subscribers, publishers increasingly maintain an online portal, where subscriptions can be managed and data practices viewed and controlled. The appropriate choices for customer interaction may differ depending on a particular magazine's audience and characteristics.

Magazine media data practices evolve with technology and consumer expectations and the Administration's approach to a data privacy framework likewise should be adaptable in an innovative marketplace. The recommended reasonableness standard in the attached comments, a concept already recognized in the NTIA's request for comment, would enable marketplace flexibility and innovation, while maintaining the fundamental privacy protection goal for consumers. This reasonableness standard is consistent with existing US privacy laws, including the Gramm-Leahy-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), as well as principles previously articulated by the Federal Trade Commission.

As detailed in the coalition comments, a reasonableness standard could assess: (i) consumer harms and benefits, (ii) the objective expectation of a reasonable consumer, and (iii) the relevant risk management practices of an organization. While some data practices could be readily classified as *per se* unreasonable or reasonable, further actions by regulators will yield increased clarity regarding specific data practices.

II. A Federal Framework and Legislation will Benefit Both Consumers and Businesses

MPA, along with other associations, has previously expressed support for a national standard for data breach legislation. The need for a Federal data privacy framework and standard is even stronger following the passage of the *California Consumer Protection Act* (CCPA). The hurried nature of CCPA deliberations, which passed in a matter of days in response to a ballot referendum deadline, did not allow for a measured and considered approach to privacy such as the approach articulated by the NTIA. Under the CCPA, all businesses—including magazine

publishers—face difficult-to-implement, costly requirements and significant legal exposure without improving privacy outcomes for consumers. We have concerns in several areas.

a. Transparency:

We agree with NTIA's assessment that 'users should be able to easily understand how an organization collects, stores, uses and shares their personal information." Magazine publishers consistently strive to effectively communicate our data practices to our customers. We also understand the NTIA's concerns that 'lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding." The CCPA creates a long list of new disclosure requirements that will significantly add to the length of privacy policies without evidence that such disclosures will improve consumer understanding of data practices.

b. Private Right of Action:

One of the most chilling provisions of the CCPA is the private right of action. In the event of a data breach, the CCPA would allow damages up to $750 per consumer per incident, or actual damages, whichever is greater. The CCPA does not require that consumer financial harm be demonstrated. As a result, business with data from 100,000 California consumers, for instance, could face damages of $75 million for a data breach that does not cause consumer harm. This level of risk will incentivize companies to settle litigation regardless of the merits of a particular case, diverting funds from beneficial consumer uses. A federal standard that accounts for consumer harm could protect consumers without risking the very existence of data-intensive businesses.

c. Unintended Cybersecurity and Fraud Risks:

Several consumer rights prescribed under the CCPA—including the rights to data access and deletion of data—will likely require businesses to combine information from various data systems and entities to respond to consumer access requests. As a result, businesses may be forced to store large amounts of consumer data in one place, which increases the risk of cyberattacks and fraud and the consequences of a data breach. The accumulation of data and new rights to access that data will provide hackers and fraudsters an increasingly tempting target, with severe potential consequences to businesses.

III. The Federal Trade Commission is the Appropriate Authority to Oversee Consumer Privacy Enforcement

The Federal Trade Commission (FTC) has a long history of examining data privacy issues, issuing guidance, and taking enforcement actions under its existing authority. With this base of knowledge and practical application, MPA believes that the FTC—which has brought hundreds of privacy and data security enforcement actions—is the appropriate federal agency to enforce consumer privacy under the Administration's risk-based approach and achieve its desired

privacy outcomes. In addition to law enforcement expertise, the FTC has time-tested experience developing practical guidance and resources for both consumers and businesses.

* * * * * * * * * *

We thank the NTIA for providing this opportunity to submit comments on behalf of our membership. We support the NTIA's goal of a risk management approach that "affords organizations flexibility and innovation in how to achieve" the desired privacy outcomes. The Administration's framework should be developed through a measured approach that is informed by all impacted stakeholders, and should incorporate a reasonableness standard for Congress to enact into law. Our organization is committed to working with the NTIA as it assesses its approach to consumer privacy. If you have any questions regarding these comments, please feel free to contact us at rcohen@magazine.org or mhenry@magazine.org or 202-296-7277.

Sincerely,

Rita Cohen
SVP, Legislative and Regulatory Policy

Mary Holland Henry
VP, Government Affairs

November 9, 2018

Submitted Via Email: privacyrfc2018@ntia.doc.gov

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

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

To Whom It May Concern:

The undersigned associations represent thousands of companies that innovate and compete in data-driven industries, and which for decades have been leaders in consumer privacy matters. As a result of our members' experience working with and helping shape privacy regimes across different industry sectors in the United States and abroad, we know firsthand the benefits and drawbacks of the various approaches to privacy regulation. As such, we appreciate the opportunity to provide the National Telecommunications and Information Administration ("NTIA") feedback on its Request for Comment ("RFC"). Outlined below are the concepts and approach we believe are best suited to create lasting protections for consumers and foster a competitive and innovative marketplace.[1]

History has shown that consumers benefit from thoughtful and measured approaches to privacy. For example, the existing privacy regulatory framework, based in part on the concepts of transparency and choice, has enabled tremendous growth and innovation in the modern economy while protecting consumer privacy and giving consumers meaningful options for how data about them will be used. Myriad consumer benefits, whether in the form of free or low cost services supported by advertising, or personalized services that deliver the right product or information at the right time, have transformed our daily lives in countless ways. New rules at the state level, however, are now threatening to disrupt this framework and fragment the marketplace. As such, we believe that the time is ripe for federal action on privacy that better reflects the interests of consumers and innovators, and our national economy.

To help drive forward the conversation about the next generation of privacy standards, we provide in these comments a high-level overview of a new privacy regulatory approach—the New Paradigm—that can help regulators, consumers, and market participants determine the merits and appropriate treatment of various data practices. We encourage the NTIA to consider the New Paradigm and the guiding principle of reasonableness, which already is implicit in many current U.S. privacy laws, as the Administration charts its approach to consumer privacy.

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

Similarly, we encourage the NTIA to address the emerging fragmentation in state privacy laws. If inconsistent approaches at the state and local level are not harmonized, such laws will create patchwork regulation of the Internet that consumers will not understand and that will not serve their interests.

In support of the NTIA's decision-making process and its activities, we recommend that the Administration prioritize and conduct a cost-benefit analysis of proposed privacy frameworks and competing state solutions, including an analysis of the economic impact of the California Consumer Privacy Act ("CCPA") and the European Union's General Data Protection Regulation ("GDPR"). Such an analysis would be timely and would help inform lawmakers, consumers, and industry of the impact of various data privacy proposals on consumers and the economy.

A NEW PRIVACY PARADIGM

Evaluating data practices based on their reasonableness should be a foundational point in any new national privacy standard regarding the collection or use of data. Under the New Paradigm, unreasonable data practices should be specifically prohibited, while reasonable data practices should be expressly permitted and encouraged.

Data practices should be assessed holistically through a reasonableness standard that could weigh, for instance: (i) the consumer harms and benefits, (ii) the objective expectation of a reasonable consumer; and (iii) the relevant management and risk mitigation practices of an organization (*e.g.*, transparency, choice, downstream contractual protections, data security, and adherence to self-regulatory standards). Many data practices, or categories of data practices, could be classified as either *per se* unreasonable or *per se* reasonable and any remaining non-classified practices could be analyzed using the factors described above. As the New Paradigm matures and is applied by regulators, consumers and businesses will gain increasing clarity regarding the treatment of data practices that are not clearly *per se* reasonable or unreasonable.

The New Paradigm's proposed reasonableness test is an expansion upon current domestic and foreign privacy laws and standards. The Federal Trade Commission's ("FTC") 2012 staff report on privacy, for instance, makes specific allowances for a company's collection and use of data in a manner consistent with the context of the transaction or with the company's relationship with the consumer, noting that a company does not need to provide consumer choice in these circumstances. Similarly, the Gramm-Leach-Bliley Act ("GLBA") includes the concept of reasonableness when it provides specific allowances for the use of nonpublic personal information. The Fair Credit Reporting Act ("FCRA") also enshrines a reasonableness-like standard through its allowance of permissible purposes for the use of consumer reports. Inherent in the FTC staff report, the GLBA, the FCRA, and other U.S. privacy laws and standards is the recognition that reasonable data practices should be specifically allowed by law and unreasonable practices should be prohibited. This concept also aligns with some elements of the

GDPR, which recognizes an organization's legitimate interests as a lawful basis for processing personal data.

A BALANCED APPROACH TO ACHIEVE CONSUMER PROTECTION AND NATIONAL PROSPERITY CONSISTENT WITH THE NTIA'S GOALS

As a general matter, the NTIA has asked for comments on a set of "privacy outcomes" that are grounded in a "risk-based approach" and that are "reasonable and appropriate for context." The New Paradigm helps achieve these outcomes by requiring the evaluation of data practices for reasonableness, which will likely include both a review of the risks related to the data practice and the context in which the data practice occurs. In effect, the New Paradigm's reasonableness categories and factors help establish and support core concepts put forward by the NTIA.

The New Paradigm also aligns with the NTIA's request for a risk management approach that "affords organizations flexibility and innovation in how to achieve these outcomes," without creating a loophole for bad actors to exploit. Consistent with the NTIA's proposed approach, and an improvement over the CCPA and the GDPR, the New Paradigm does not create a one-size-fits-all privacy standard for every piece of data or for every kind of data practice regardless of risk, context, or the sensitivity of the data. Such an inflexible approach creates major barriers to entry for new market participants because it raises the risks and costs of holding data, even when privacy harms are remote. The New Paradigm instead provides a set of factors a company can use to evaluate its data practices that is tailored to its circumstances and customer relationships, thereby establishing a regulatory standard under which all companies, large or small, and across industries can thrive.

In keeping with the NTIA's goals, to ensure the successful implementation of a national privacy standard that provides strong consumer protections and that reduces regulatory fragmentation, we recommend that the FTC enforce the concepts underlying the New Paradigm as a single national standard, which supersedes state privacy laws.

* * *

We encourage the NTIA to consider the concepts underlying the New Paradigm, and the guiding principle of reasonableness, to help refocus the privacy discussion on how to create lasting protections for consumers in a modern, data-driven economy. The NTIA should also work to prevent the emerging regulatory fragmentation at the state level, and advocate for the adoption of a national standard that is more rational, effective, and productive for both consumers and market actors.

Finally, we believe that the Administration is well positioned to provide a cost-benefit analysis of the impact of proposed privacy frameworks and emerging state laws. We hope the

Administration will leverage its capabilities to conduct these assessments to help consumers, lawmakers, and industry understand the impact of various data privacy proposals.

We look forward to working with the Administration to ensure that the United States remains at the forefront of innovation and consumer protection. If you have questions, please contact any of the undersigned or Stu Ingis at SIngis@Venable.com or (202) 344-4613.

Respectfully submitted,

Association of National Advertisers
American Association of Advertising Agencies
American Advertising Federation
Association of Magazine Media
Consumer Data Industry Association
Insights Association
Interactive Advertising Bureau
National Business Coalition on E-Commerce and Privacy
Network Advertising Initiative
Software & Information Industry Association