BEFORE THE

HOUSE OF REPRESENTATIVES SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE OF THE COMMITTEE ON ENERGY AND COMMERCE

HEARING ON

PROTECTING CONSUMER PRIVACY IN THE ERA OF BIG DATA

FEBRUARY 26, 2019

TESTIMONY OF

DAVID F. GRIMALDI, JR.

EXECUTIVE VICE PRESIDENT, PUBLIC POLICY

INTERACTIVE ADVERTISING BUREAU

Chairwoman Schakowsky, Ranking Member Rodgers, and Members of the Committee, thank you for the opportunity to testify today. I am Dave Grimaldi, Executive Vice President for Public Policy at the Interactive Advertising Bureau ("IAB"). Founded in 1996 and headquartered in New York City, the IAB represents over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns. Together, our members account for 86 percent of online advertising in the United States.

Working with our member companies, the IAB develops technical standards and best practices, conducts critical research on interactive advertising, and educates brands, agencies, and the wider business community on the importance of online marketing to digital trade. I am honored to discuss with you today the important work that IAB and its members are engaged in to support consumer privacy while helping businesses of all sizes succeed online. We believe the time is right for a new, federal paradigm on consumer privacy that sets clear rules that describe which data practices are permitted and prohibited, and that distinguishes between data practices that pose a threat to consumers and those that do not. This is a critical moment for Congress to step in and prevent the country from ending up with a patchwork of ambiguous and inconsistent state laws that will create uncertainty for business and uneven protections for consumers. We look forward to working with the Committee to set a national data standard that works for consumers and businesses alike.

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

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising 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, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.[1] 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.[2] 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.

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to

[1] 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.
[2] *Id.*

valuable content, or the ability to create their own platforms to reach millions of their fellow citizens. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are 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. Indeed, as the Federal Trade Commission ("FTC") noted in its recent comments to the National Telecommunications and Information Administration, 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 and that will become available in the future.[3]

II. IAB Members Have Long Supported Strong Consumer Privacy Protections

The IAB and its members have been at the forefront of promoting responsible data practices, and consumer trust is vital to our member companies' ability to operate successfully in the marketplace. The Internet's framework made customer relationships the core asset of every successful enterprise, and data is replacing legacy assets like a company's manufacturing footprint or access to raw physical materials. The success of a business is premised on having personalized relationships with millions of consumers at scale, and that is best achieved only when companies responsibly use the information that customers have provided about themselves. Such data is the key driver of companies' growth, ability to reach individuals at scale, and creation of consumer value in the modern digital age. Consumers expect and appreciate the

[3] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

tailored experiences that are possible using data. We strongly believe that businesses can address consumer concerns by preventing harmful and unexpected uses of data while preserving beneficial ones.

This commitment to consumer trust, and recognition that data is essential for business success, is best exemplified through IAB's integral role in the creation of the self-regulatory systems administrated by the Digital Advertising Alliance ("DAA"). The DAA is an industry body convened a decade ago to create a self-regulatory code for all companies that collect or use data for interest-based advertising online, based on practices recommended by the FTC in its 2009 report on online behavioral advertising.[4] The rules set by the DAA have continued to evolve in the intervening years to account for new data practices.

Today, the DAA Principles provide consumer transparency and control regarding data collection and use of web viewing data, application use data, precise location data, and personal directory data.[5] The DAA Principles also contain strong prohibitions on the use of such data for eligibility purposes for employment, insurance, credit, and healthcare treatment,[6] and detailed guidance around the application of the Principles in the mobile[7] and cross-device[8] environments. Most recently, to provide users with increased transparency about the source of the political advertising they see online, the DAA released guidance on the application of the Principles of

[4] DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009) http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.
[5] DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009) http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; DAA, *Self-Regulatory Principles for Multi-Site Data (MSD)* (Nov. 2011) http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf; DAA, *Application of Self-Regulatory Principles to the Mobile Environment*, (Jul. 2013) http://www.aboutads.info/DAA_Mobile_Guidance.pdf.
[6] DAA, *MSD*, 4-5 (Nov. 2011); DAA, *Application of Self-Regulatory Principles to the Mobile Environment*, 31-32 (Jul. 2013).
[7] DAA, *Application of the Self-Regulatory Principles to the Mobile Environment* (Jul. 2013).
[8] DAA, *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015).

transparency and accountability to political advertising.[9] Importantly, the YourAdChoices Program and the DAA Principles are a novel kind of industry-led initiative whereby *all* companies engaging in the covered practices are subject to established privacy safeguard obligations. The DAA Principles are independently monitored and enforced by accountability programs. To date, more than 90 compliance actions have been publicly announced, and additional investigations have occurred without being made public.

One of the innovations of the DAA program has been the DAA's YourAdChoices Icon (). This icon is served in or near ads over a trillion times per month worldwide in order to provide transparency outside of the privacy policy. By clicking this icon in any ad, consumers can see more information about interest-based advertising and can access simple, one-button tools to control the future collection and use of data for interest-based advertising. Consumer awareness and understanding of the program continues to increase, and a 2016 study showed more than three in five consumers (61 percent) recognized and understood what the YourAdChoices Icon represents.[10]

The effectiveness of the DAA Self-Regulatory Program also has been recognized by the United States government. At a 2012 White House event, Obama Administration officials including the then-FTC Chairman and then-Secretary of Commerce publicly praised the DAA's cross-industry initiative. The DAA's approach has also garnered kudos over time from the leadership at the FTC and from FTC staff for the program's pioneering privacy work.[11]

---

[9] DAA, *Application of Self-Regulatory Principles of Transparency & Accountability to Political Advertising*, (May 2018).
[10] DAA, *Consumers' recognition of the AdChoices Icon -- and understanding of how it gives choice for ads based on their interests -- continues to rise* (Sep. 29, 2016) https://digitaladvertisingalliance.org/blog/icon-you-see-yeah-you-know-me-0.
[11] The White House recognized the Self-Regulatory Program as "an example of the value of industry leadership as a critical part of privacy protection going forward." The DAA also garnered kudos from then-Commissioner Maureen Ohlhausen who stated that the DAA "is one of the great success stories in the [privacy] space." In its cross-device tracking report, the FTC staff also

III. The Existing U.S. Privacy Framework Should be Updated

The time is right for the creation of a new paradigm for data privacy in the United States. IAB, working with Congress, and based on our members' successful experience creating privacy programs that consumers understand and use, can achieve a new federal approach that, instead of bombarding consumers with notices and choices, comprehensively describes clear, workable, and consistent standards that consumers, businesses, and law enforcers can rely upon. Without a consistent federal privacy standard, a patchwork of state privacy laws will create consumer confusion, present substantial challenges for businesses trying to comply with these laws, and fail to meet consumers' expectations about their digital privacy. We ask the Congress to standardize privacy protections across the country by passing legislation that provides important protections for consumers while allowing digital innovation to continue apace.

We caution Congress not to rely on the frameworks set forth in Europe's General Data Privacy Regulation ("GDPR") or California's Consumer Privacy Act ("CCPA") as examples of the ways in which a national privacy standard should function. These frameworks are not new approaches, only more restrictive versions of the existing privacy paradigm. While well-intentioned, their rigid frameworks impose significant burdens on consumers, such as rampant over-notification leading to consent fatigue in consumers and creating an indifference to important notices regarding their privacy. At the same time, these regimes fail to stop many practices that are truly harmful to consumers. These laws also display a misguided antagonism

praised the DAA for having "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."

toward online advertising, and fail to recognize the various ways in which digital advertising subsidizes the rich online content and services that consumers want.

Far from being a desirable model, the GDPR shows how overly restrictive frameworks can be harmful to competition and consumers alike. Less than a year into the GDPR's applicability, the negative effects of its approach have already become clear. Following the GDPR's enforcement date, the volume of programmatic advertising in Europe dropped between 25 and 40 percent across exchanges.[12] The GDPR has also directly led to consumers losing access to online resources, with more than 1,000 U.S.-based publishers blocking European consumers from access to online material in part because of the inability to profitably run advertising.[13] At least one major U.S. newspaper is charging European subscribers an additional $30 to access its online content because of an inability to run effective and profitable advertising in that market.[14]

Small businesses and startups also saw the negative impact of the GDPR, with many choosing to exit the market. Prior to the GDPR's enforcement date, according to media reports, some smaller companies in the United States chose to leave the European market instead of risk the fines related to potential GDPR violations.[15] Over the time the GDPR has been in effect, some academic research estimates that startup investments in European companies have dropped

[12] Jessica Davies, DigiDay, *GDPR mayhem: Programmatic ad buying plummets in Europe (*May 25, 2018) https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/.
[13] Jeff South, Nieman Lab, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect* (Aug 7, 2018) http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.
[14] 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/.
[15] Ivana Kottasová, CNNBusiness, *These companies are getting killed by GDPR* (May 11, 2018) https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html; 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.

40 percent in aggregate.[16] These examples show the clear imbalance that the GDPR strikes between innovation and privacy.

The GDPR and CCPA fail to achieve their stated goals in a multitude of ways. The GDPR, for example, places inflexible requirements on businesses in the name of consumer privacy, but falls short of giving consumers real and effective rights and choices. Consent banners and pop-up notices have been notably ineffective at curbing irresponsible data practices or truly furthering consumer awareness and choice. The CCPA follows in the footsteps of the GDPR and could harm consumers by impeding their access to expected tools, content, and services; revealing their personal information to unintended recipients due to the lack of clarity in the law; and allowing unregulated third parties to access personal information under the guise of facilitating consumer requests. In addition, the CCPA's unclear drafting has created a level of uncertainty that has some businesses questioning whether they will be forced to refrain from doing business in California altogether – a move that some companies have already taken in Europe in response to the GDPR. The United States should, therefore, learn from the lessons of the GDPR and CCPA by creating a new paradigm for privacy protection that offers clarity and flexibility, both of which are critical to effective privacy protection.

Congress should look to a new paradigm for digital privacy that will not threaten the goods and services that consumers seek on the Internet. Consumers rely on the ad-supported model to enjoy the Internet's free content and services. Consumers understand and support the exchange of value in which data-driven advertising funds the free or reduced cost online services

[16]Mark Scott *et al*., *Six months in, Europe's privacy revolution favors Google, Facebook* (Nov. 23, 2018) https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/.

they receive. In fact, a DAA-commissioned Zogby survey found that consumers attributed a value of nearly $1,200 a year to common online ad-supported services, like news, weather, video content, and social media.[17] A large majority of surveyed consumers (85 percent) like the ad-supported model, and 75 percent said they would greatly decrease their use of the Internet were they required to pay hundreds of dollars a year for currently free content.[18] The new federal privacy standard should take into account the fact that consumers overwhelmingly value and want to keep their access to ad-supported online resources.

An effective new paradigm also should shift the burden of privacy compliance away from consumers. Consumers want to know their privacy is protected, but they cannot spend hours every day finding, reading, and interpreting privacy notices, as regimes like the GDPR and CCPA envision. Instead, Congress should develop clear rules that describe which data practices are permitted and prohibited. Just as when rules for automobile safety were developed, consumers should be able to look to Congress to create reasonable, responsible, and sensible standards to protect their privacy in a smart way.

To achieve these goals, the IAB asks Congress to support a new paradigm that would follow certain basic principles. First, in contrast to many existing privacy regimes, a new law should impose clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified in the law. Consumers will then be protected from such practices without the need for any action on their part. Second, a new law should distinguish between data practices that pose a threat to consumers and those that do not, rather than taking a broad-brush

[17] Zogby Analytics, *Public Opinion Survey On Value Of The Ad-Supported Internet* (May 2016) https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.
[18] *Id.*

approach to all data collection and use. Third, the law should incentivize strong and enforceable compliance and self-regulatory programs, and thus increase compliance, by creating a rigorous "safe harbor" process in the law. And finally, it should reduce consumer and business confusion by preempting the growing patchwork of state privacy laws.

IAB asks for the Congress's support in developing such a framework to enhance consumer privacy. Thank you for your time today. I welcome your questions.

* * *