BEFORE THE

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

HEARING ON

POLICY PRINCIPLES FOR A FEDERAL DATA PRIVACY FRAMEWORK IN THE UNITED STATES

FEBRUARY 27, 2019

TESTIMONY OF

RANDALL ROTHENBERG

CHIEF EXECUTIVE OFFICER

INTERACTIVE ADVERTISING BUREAU

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, I am honored for the opportunity to testify today. I am Randall Rothenberg, Chief Executive Officer of the Interactive Advertising Bureau. Founded in 1996 and headquartered in New York City, the IAB represents over 650 leading media and technology companies, and consumer brands that are responsible for selling, delivering, and optimizing digital marketing campaigns. Together, our members account for the vast majority of digital advertising in the United States. Working with our member companies, the IAB develops technical standards and best practices to create efficient, effective, and safe digital marketing environments, trains industry professionals on these standards and practices, and fields critical research on the role of interactive marketing in growing brands, companies, and economies. I have had the honor of testifying before Congress several times on the topic of privacy in digital media and advertising environments, and each time I offer up the same guidance and the same solutions. I am going to repeat myself once again, if with a bit more urgency, because I believe there is a ready path forward to assure both the safety of consumers and continued growth in the consumer economy.

The Internet is perhaps the most powerful and empowering mode of communication and commerce ever invented. It is built on the exchange of data between individuals' browsers and devices, and myriad server computers operated by hundreds of millions of businesses, educational institutions, governments, NGOs, and other individuals around the world. Advertising has served an essential role in the growth and sustainability of the digital ecosystem almost from the moment the first Internet browsers were released to the public in the 1990s. In the decades since, data-driven advertising has powered the growth of e-commerce, the digital news industry, digital entertainment, and a burgeoning consumer-brand revolution by funding innovative tools and services for consumers and businesses to connect, communicate, and trade.

Data-driven advertising is not an Internet phenomenon; it has been a fundamental part of American business for well more than a century. But never in history has the open flow of data fueled such entrepreneurial and creative vigor, generating untold consumer benefit by enabling access to free content, services, and connectivity across once-insurmountable boundaries.

But these enormous benefits come at a price, and that is what we are here to address today. The source of the Internet's innovation is also the source of its vulnerabilities: an open, porous supply chain that allows any actor, no matter how creative or how corrupt, to plug and play - to invent a new business or poison a culture. The data exchanges that power new businesses and drive unprecedented cultural invention can also be used to violate consumers' security and privacy. The question before Congress is: How do we close off the sources of corruption and reduce the hazards without impeding the innovation?

This is no easy task. The economy is in the midst of an enormous shift; data increasingly is the core asset of every enterprise, replacing such legacy assets as a company's manufacturing footprint or its access to raw materials. The greatest legacy consumer brands of the 20th Century are being challenged by thousands of upstart brands in every category, which share one trait: regardless of whether they make luggage, eyeglasses, underwear, or beer, their success is premised on having individual relationships with millions of consumers. This is achieved only through the responsible use of data. Customer relationships are improved across all industries by operationalizing consumer data. Such data is the essential driver of companies' growth, their ability to reach individuals at scale, and their creation of consumer value.

Central to companies' data-fueled growth is trust. As in any relationship, from love to commerce, trust underlies the willingness of parties to exchange information with each other,

and thus their ability to create greater value for each other. The equation is simple: The economy depends on the Internet; the Internet runs on data; data requires trust. IAB strongly believes that legislative and regulatory mechanisms can be deployed in ways that will reinforce and enhance trust in the Internet ecosystem.

But in doing so, we must remain cognizant of the ways the economy – the pre-digital as well as the digital economy – have used data to foster growth, and strive not to disrupt the many legitimate means consumer data has been used to fuel innovation, economic growth, education, social organization, and culture. IAB, our members, and our sister trade associations stand ready to work with Congress to help craft a legislative and regulatory regime that protects consumers, while avoiding the unintended consequences that can result from ill-considered regulatory regimes, notably the erection of barriers to market entry, the erosion of competition, and reinforced advantage for the largest incumbents.

We recommend Congress start with a premise that for most of American history was self-evident, but today seems almost revolutionary: consumer data is a good thing. It is the raw material of such essential activities as epidemiology, journalism, marketing, business development, and every social science you can name. The United States recognized the centrality of consumer data to the growth of this nation back in 1790, when we conducted the first census, and reinforced that centrality to the U.S. economy in 1902, when the Congress placed the Census Bureau under the auspices of the newly formed Department of Commerce and Labor. New data science and digital tools do not change the fact that data-based marketing is a reasonable and safe practice that has long been supported by the government. Fostering new private sector uses of data is a net good for consumers and the country that should not be curtailed through badly constructed controls.

Nor should we ignore the fact that something needs to be done by the Federal Government. As I appear before you today, the digital marketing and media ecosystem is at a crossroads. Recent events such as the Facebook-Cambridge Analytica scandal have placed a spotlight on companies' need to responsibly, safely, and transparently manage and use consumers' data, and make consumer privacy and security the foundational requirement for doing business in the modern economy. In response to those events, California, Washington, and other states are advancing new requirements and restrictions on businesses. These laws are well meaning and I support their intended goals. Nevertheless, elements of these proposals are reactive and risk stifling what should be understood as a uniquely American technological advantage. As a result, due to the emergence of conflicting state law regimes, consumer privacy has quickly become an area that needs federal leadership and engagement.

Uniquely among today's speakers - and, I believe, any other witnesses you may call before you - the IAB and our trade association partners have the ability to provide Congress with a guide based on our experience building effective mechanisms to protect consumer privacy and security, such as the Digital Advertising Alliance's ("DAA") YourAdChoices and PoliticalAds programs that provide consumers with transparency, control, and accountability in their digital advertising experience,[1] and the Trustworthy Accountability Group ("TAG"), the organization that protects consumers and businesses alike from fraudulent digital advertising, malware, and ad-supported piracy.[2] While hundreds of companies have signed on to these programs, and even nonparticipators have faced enforcement actions, by force of law, Congress is best able to ensure the broadest level of compliance. Consequently, our industry is heartened by the federal

[1] *See* www.youradchoices.com; www.aboutpoliticalads.org.
[2] *See* www.tagtoday.net.

government joining us in our longstanding effort to enhance consumer privacy and security. In fact, if Congress were to give our programs the force of law tomorrow, building on our work and going further, many consumer privacy and security concerns would be mollified almost immediately.

Consequently, we believe our goals align with the Congress' decision to take a proactive position on data privacy, rather than the reactive approach that has been adopted by Europe and some states. We believe we can work together as partners in this effort with you to advance consumer privacy. Our model is the partnership between government and industry that created the modern concept of automotive safety in the 1960s. Yes, the partnership began as a shotgun wedding. Yes, the auto industry resisted at first. But an undeniable consumer right – to be safe on the highways – met well-researched solutions, which the Congress embedded in well-crafted laws that were supported by the states. The result has been millions of lives and billions of dollars saved. We believe the analogy holds well here. Americans have a right to be secure on the information superhighway. Well-researched solutions and well-crafted laws can assure their "digital wellness." We should be thorough, practical, and collaborative. Our goal should be to find the three or five or ten practices and mechanisms – the seat belts and air bags of the Internet era - that companies can implement and consumers can easily adopt that will reinforce privacy, security, and trust.

To begin, we believe it is vital that government, industry, and consumer organizations establish a new paradigm for data privacy in the United States, based on strong principles and underpinned by mechanisms to achieve those principles. Together, based on our members' experience, we can achieve this new paradigm by developing a federal privacy law that, instead of bombarding consumers with notices and choices, comprehensively provides clear, even-

handed, consistent, and predictable rules of the road that consumers, businesses, and law enforcers can rely upon. Without a consistent, preemptive federal privacy standard, the patchwork of state privacy laws will create consumer confusion, present significant challenges for businesses trying to comply with these laws, and ultimately fall short of consumers' expectations about their digital privacy. We ask the Congress to harmonize privacy protections across the country through preemptive legislation that provides meaningful protections for consumers while allowing digital innovation to continue apace.

In developing this new paradigm, IAB cautions the Congress from relying on legal regimes such as Europe's General Data Privacy Regulation ("GDPR") or California's Consumer Privacy Act ("CCPA") as models for how a privacy standard should function. While well-intentioned and important developments in bringing deserved attention to the issue of data privacy, these rigid frameworks impose significant burdens on consumers while failing to stop many practices that are truly harmful; they also fail to recognize the various ways in which digital advertising subsidizes the plentiful, varied, and rich digital content and services consumers use on a daily basis and have come to expect. Consumers enthusiastically embrace the ad-supported model *because of* the free content and services it enables. They are aware of and support the exchange of value in which data-driven advertising funds the free or reduced-cost services they receive. In fact, a Zogby survey commissioned by the DAA found that consumers assigned a value of nearly $1,200 a year to common ad-supported services, like news, weather, video content, and social media. A large majority of surveyed consumers (85 percent) like the ad-supported model, and 75 percent said they would greatly decrease their engagement with the Internet were a different model to take its place under a miscalibrated legal regime.[3]

[3] *See* www.digitaladvertisingalliance.org/press-release/zogby-poll.

The economic contribution of the ad-supported economy is undeniable. IAB research from 2017, conducted with Harvard Business School Professor John Deighton, found the ad-supported Internet created 10.4 million jobs. Calculating against those figures, this ecosystem contributed $1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6 percent of U.S. gross domestic product.[4] Congress should embrace a new paradigm for privacy that does not curtail these goods and services that consumers seek on the Internet.

Moreover, GDPR and CCPA appear likely to fail to achieve their stated goals. GDPR, for example, poses stringent, mechanical requirements on businesses but falls short in giving consumers real rights and choices – and does nothing to implement actual privacy and security mechanisms. Consent banners and pop-ups that were supposed to impose limits on companies have been notably ineffective at curbing irresponsible data practices or truly furthering consumer awareness and choice. Opt-ins and opt-outs, I would submit to you, are not the seat belts and air bags of the information superhighway.

The CCPA, for its part, could actually harm consumers by impeding their access to expected loyalty programs and subscription renewal messages; divulging their personal information to unintended recipients due to the lack of clarity in the law; and allowing unregulated third parties to access personal information in 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 pull out of the California market altogether – something that already has happened in Europe.[5] The United States should,

[4] *See* www.iab.com/economicvalue.

[5] Following the implementation of the GDPR, some smaller U.S.-based companies and publishers chose to exit the European market instead of risk the fines related to potential GDPR violations. 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; Jeff South, Nieman Lab, *More than 1,000 U.S. news sites are still unavailable in*

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.

Consumers want to know their privacy is protected, but they cannot spend hours every day finding and reading privacy notices. Our goal should not be to place more burdens on consumers, but to make their privacy protections reflexive, if not automatic. To start, we are asking Congress to develop clear rules about what data practices should be prohibited and what data practices should be permitted. Just as when rules for food, pharmaceuticals, and automobile safety were developed, consumers should be able to look to Congress to create reasonable, responsible, and sensible rules of the road to protect their privacy.

To achieve this goal, IAB asks for Congress' support in developing a new paradigm that would follow these 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. Second, it should distinguish between data practices that pose a threat to consumers and those that do not, rather than taking a broad-brush approach to all data collection and use. Third, it should incentivize strong and enforceable compliance programs, and thus universalize 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.

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/;. Additionally, some companies chose to charge European users more for access to content because of an inability to run effective and profitable advertising in that market. 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/.

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

* * *