

August 20, 2018

Submitted Electronically Via www.ftc.gov/ftc-hearings

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex C)
Washington, DC 20580

RE: Request for Comment on “Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201”

To Whom It May Concern:

The undersigned trade associations collectively represent thousands of companies, from small businesses to household brands, which engage in responsible data collection and use that benefit consumers and the economy. We provide these comments in response to the Federal Trade Commission’s (“Commission” or “FTC”) request for public comment on “Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201” published on June 20, 2018.¹ We and our members believe that self-regulatory models, coupled with well-reasoned sectoral laws focused on concrete consumer harm, have improved consumer protection, privacy, and security over the past twenty-plus years, and promote innovation and growth in the modern Internet-enabled economy.

Since the Commission’s 1995 hearings (“Pitofsky Hearings”), the Internet has evolved from a mere curiosity to the backbone of the modern economy. Our members, which include the leading online platforms, advertisers, marketers, data companies, and content providers, have embraced the data-driven Internet economy to engage with consumers, deliver valuable content, and create jobs across the country. Additionally, the democratizing effects of the Internet removed traditional barriers to entry for new market participants, allowing some of the world’s leading companies and brands to flourish, new companies to challenge them, and drive competition within newly-created markets. We support the FTC in its mission to ensure that free markets support innovation and growth, while also ensuring that data is collected and used responsibly within a framework of statutory rules focused on concrete consumer harms, and self-regulatory principles to encourage consumer confidence and trust in the data-driven economy. Below we discuss advances in five of the FTC’s identified areas of interest, and explain how the current framework for online data collection and use has created and driven the explosion in economic, consumer, and competitive benefits.

¹ Federal Trade Commission, *FTC Announces Hearings On Competition and Consumer Protection in the 21st Century* (June 20, 2018) <https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st>.

1) Consumer protection on the Internet has grown stronger, fostering innovation, economic growth, and consumer trust.

In the two-plus decades since the Pitofsky Hearings, the U.S. system of sectoral laws, focused on concrete consumer harms, continues to provide strong consumer protection where it is needed most. These laws focus on particular areas where the nature of the data, if misused or misappropriated, could cause discernible harm to consumers. The United States wisely took a harm-based approach to these protections, identifying areas where consumers may be harmed, and regulated those areas. For example, patient health data is protected by the Health Information Portability and Accountability Act (“HIPAA”), the use of data for credit and other eligibility purposes is protected by the Fair Credit Reporting Act (“FCRA”), the Children’s Online Privacy Protection Act (“COPPA”) protects children’s privacy on the Internet, and the Gramm-Leach-Bliley Act (“GLBA”) protects consumers’ financial data. This regulatory approach allows data to be used responsibly by companies to improve consumer experiences and fuel economic growth and competition, while providing limits on potentially harmful practices. This existing sectoral framework is a successful means of advancing innovation and competition, while also providing consumers with transparency and control over their data choices.

The FTC takes a lead role in actively enforcing some of these sectoral laws. For example, in the past few months the Commission brought actions alleging violations of its rules under COPPA and the GLBA.² The FTC’s continued, active, and vigilant enforcement efforts ensure that, where consumers could see real harm from the misuse of data, the federal government will punish bad actors by leveraging powers that are carefully calibrated by Congress through the legislative process.

In addition to new sectoral laws that came into effect to address harms identified by Congress following the Pitofsky Hearings, the private sector continued to develop effective and enforceable self-regulatory programs to supplement those laws.³ The value of these programs was identified in the report produced by the Pitofsky Hearings. In that report, the Commission stated that “[s]elf-regulation may offer some of the most promising avenues for consumer protection in this new medium [the Internet], without inhibiting its development.”⁴ The Commission’s foresight was proven correct in the online space, as seen in the FTC’s report on *Self-Regulation Principles for Online Behavioral Advertising* from 2009, and again validated in its *Cross-Device Tracking* report from 2017 when it stated that such programs improve “the level of consumer protection in the marketplace.”⁵ These programs account for new developments in the marketplace, developments that the slow pace of legislation and regulation are unable to address in a timely manner.

² *U.S. v. Prime Sites, Inc.*, Complaint for Permanent Injunction, Civil Penalty, and Other Relief, Case No. 2:18-cv-199 (D. Nev. Feb. 5, 2018); *FTC v. LendingClub Corporation*, Complaint, Case No. 3:18-cv-02454 (N.D. Cal. Apr. 25, 2018).

³ These new statutes include COPPA, HIPAA/HITECH Act, the GLBA, and amendments to the FCRA contained in the Fair and Accurate Credit Transactions Act of 2003.

⁴ Federal Trade Commission, *Anticipating the 21 Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, 31 (May 1996) https://www.ftc.gov/system/files/documents/reports/anticipating-21st-century-competition-policy-new-high-tech-global-marketplace/gc_v2.pdf.

⁵ Federal Trade Commission, *FTC Staff Report: February 2009 Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009); Federal Trade Commission, *Cross-Device Tracking: An FTC Staff Report*, 10 (Jan. 2017).

A prime example of effective, enforceable self-regulation is the Digital Advertising Alliance (“DAA”). Our trade associations came together to create the DAA in 2009 to establish and implement self-regulation for online, mobile, and cross-device data collection, use, and transfer for certain purposes. This self-regulatory framework is backed by credible and independent enforcement. The DAA’s *Self-Regulatory Principles for Online Behavioral Advertising* (“Principles”), released in 2009, implemented self-regulatory principles of transparency and control regarding data collection and use for online behavioral advertising (“OBA,” also known as interest-based advertising).⁶ These Principles are based on the FTC’s recommended self-regulatory practices.⁷ The FTC’s original recommendations recognized the need for flexibility to accommodate new technologies while continuing to provide for privacy-protective practices. Specifically, FTC “[s]taff supported self-regulation because it provides the necessary flexibility to address evolving online business models,” and the Principles take the lead in this approach.⁸ We consider the DAA’s focus on providing consumers with meaningful transparency and control over the collection, use, and transfer of data to be the model for how various stakeholders in the Internet ecosystem can come together to think about consumer privacy and create flexible and workable solutions.

The Principles are composed of seven core principles, which call for consumer education, the provision of choice mechanisms, data security, heightened protection for certain sensitive data, consent for certain material changes to data collection and use policies, and strong enforcement mechanisms. To increase consumer notice, the Principles require enhanced notice outside of the privacy policy so that consumers can be made aware of the companies they interact with while using the Internet. The Principles help to increase consumer trust and confidence in how information is gathered from consumers online, and how that value exchange is used to deliver advertisements based on their interests to provide the free and low-cost services they enjoy.

The DAA program continues to evolve to keep pace with change in technology and the manner by which consumers engage with digital content. In 2011, the DAA evolved the Principles to apply to the collection and use of Multi-Site Data collected from a particular computer or device regarding Web viewing information over time and across non-affiliated Web sites for certain uses.⁹ Then, in 2013, to address the rise of mobile devices, DAA again produced guidance to address how the Principles apply to the collection and use of data from mobile devices, including Cross-App Data, Precise Location Data, and Personal Directory Data.¹⁰ For Precise Location Data, the Principles require companies to acquire user consent for the collection, use, and transfer of such data for DAA-covered purposes, and provide a means by which consumers can withdraw their consent. In 2015, the DAA released guidance for the

⁶ Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009).

⁷ Federal Trade Commission, *FTC Staff Report: February 2009 Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009).

⁸ *Id.*

⁹ Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data* (Nov. 2011) (hereinafter *MSD Principles*).

¹⁰ Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (Jul. 2013) (hereinafter *Mobile Guidance*).

application of the Principles to the collection and use of data across devices.¹¹ Most recently, the DAA announced the PoliticalAd Program to help bring transparency and accountability to digital political advertising.¹² The Principles and the DAA program as a whole are a proven and effective structure to manage the various aspects of the collection and use of data that can grow with the marketplace as new technology is introduced, and as consumers grow to expect new and novel services. This technology-neutral framework is capable of balancing consumers' interests in transparency and control with their desire to access innovative products and services in the marketplace. These Principles also allow companies to compete in the digital marketing ecosystem based on a common understanding of how the market should function.

Since the release of the initial self-regulatory principles in 2009, the program has grown in participation rates to over hundreds of leading companies and thousands of brands. Additionally, the DAA's various digital properties have reached 80 million consumers. The centerpiece of the DAA program is the YourAdChoices Icon  ("Icon"), a universal symbol deployed within or near advertisements delivered through DAA-covered practices, or on Web sites and mobile applications where data is collected or used for DAA-covered purposes. More than three in five consumers (61%) reported in a 2016 study that they recognized the Icon and understood what it represents.¹³ The Icon appears more than a trillion times per month worldwide across the digital marketplace. By clicking on the Icon, consumers are brought to a clear disclosure regarding the participating company's data collection and use practices, as well as an easy-to-use mechanism to opt out of further data collection and use for OBA.

We also recognize that strong, independent enforcement is the key to any self-regulatory program. Compliance with the DAA Principles is monitored and enforced by two accountability programs.¹⁴ The Council of Better Business Bureaus' program has brought more than 85 public enforcement actions, and issued several compliance warnings, which dealt with desktop, mobile, native advertising, non-cookie based data collection technologies, cross-device linking, and video advertising.¹⁵ The breadth of the accountability program's actions show the responsive nature and enforceability of the DAA's program. This program is recognized by the FTC as a self-regulatory program with "teeth."¹⁶

The successful self-regulatory approach taken by the DAA led to a February 2012 event at the White House with senior administration officials, including the then-Chairman of the FTC and the then-Secretary of Commerce. Those officials acknowledged the DAA's program as "an

¹¹ Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015).

¹² Digital Advertising Alliance, *Application of the Self-Regulatory Principles of Transparency & Accountability to Political Advertising* (May. 2018).

¹³ Digital Advertising Alliance, *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>.

¹⁴ See Council of Better Business Bureaus, *Accountability Program Decisions, Dispositions, Closures, and Guidance* (2018), <http://www.ascreviews.org/accountability-program-decisions/>; Data & Marketing Association, *Ethics & Compliance* (2018) <https://thedma.org/accountability/ethics-and-compliance/>.

¹⁵ *Id.*

¹⁶ Remarks of FTC Chairman Jon Leibowitz at White House Privacy Event (Feb. 23, 2012) <http://www.ftc.gov/speeches/leibowitz/120223whitehouse-privacy.pdf>.

example of the value of industry leadership as a critical part of privacy protection going forward.”¹⁷ The DAA also received kudos in 2013 from Commissioner Maureen Ohlhausen stating that the DAA “is one of the great success stories in the [privacy] space.”¹⁸ In its *Cross-Device Tracking* report, the FTC staff stated, “...DAA [has] 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.”¹⁹

This decade-plus cooperative and effective system of sectoral laws and industry self-regulation allowed the data-driven, ad-supported Internet economy in the United States to deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem* conducted for the Interactive Advertising Bureau (“IAB”) by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.²⁰ Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, which is double the 2012 figure and accounts for 6% of U.S. gross domestic product.²¹ The study, designed to provide a comprehensive review of the 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 and the competition that it engenders. These benefits flow directly from the strong, effective, and time-tested privacy framework of the United States.

Consumers, not just industry, embrace the ad-supported model of the Internet and use it to create value in all areas of life, whether through e-commerce, free access to valuable content, or the ability to exercise their right to free speech and expression. They are increasingly aware that the data collected about their interactions and behavior on the Internet, and in mobile applications, is then 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. In a Zogby survey commissioned by the DAA, consumers assigned the value of the ad-supported services, like news, weather, video content, and social media, to be \$99.77 per month, or \$1,197 a year.²² A large majority of surveyed consumers, 85%, stated they like the ad-supported model, and 75% indicated that they would greatly decrease their engagement with the Internet if a different model were to take its place.²³

¹⁷ Speech by Danny Weitzner, *We Can’t Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age* (February 23, 2012), available at <http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age>.

¹⁸ Katy Bachman, *FTC’s Ohlhausen Favors Privacy Self-Regulation*, Adweek (June 3, 2013), available at <http://www.adweek.com/news/technology/ftcs-ohlhausen-favors-privacy-self-regulation-150036>.

¹⁹ Federal Trade Commission, *Cross-Device Tracking: An FTC Staff Report*, 10 (Jan. 2017).

²⁰ John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) (hereinafter *Value of Data*) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

²¹ *Id.*

²² Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016) http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf.

²³ *Id.*

2) The use of big data in a responsible and privacy-conscious manner drives increased competition.

As explained above, the explosive growth of the data-driven Internet economy is fueled by data. Data-driven marketing allows even the smallest and newest companies to reach consumers that may be interested in their products and services at a scale that was previously available to only the most established and largest companies. With access to “big data,” companies of all sizes and resources are able to reach consumers across the country and around the globe in seconds, immediately placing smaller companies in the marketplace with equal access to consumers as its competitors.

This data-driven advertising activity is done in a responsible manner within the established framework of sectoral laws, enforceable self-regulation, and the Commission’s authority under Section 5 of the FTC Act, thereby ensuring consumer privacy is respected. Companies that leverage data-driven marketing know that consumer trust is paramount to continued consumer engagement. This drives compliance with the various “rules of the road” for digital marketing, and causes the industry to continue to evolve those rules to meet consumer demand. This evolution is evident in the founding and continued development and growth of the DAA. As new uses of digital advertising data emerge, and consumer expectations shift, so do the industry’s principles and guidelines to allow them to express their preferences.

Not only does the ad-supported, data-driven Internet benefit competition and businesses, consumers reap the greatest reward in access to low-cost and free content, services, and platforms for expression. As the DAA’s Zogby survey shows, consumers place immense value on the services that advertising supports.²⁴ Additionally, the low cost of entry for companies means that consumers have near endless choice regarding which services they patronize. The low friction nature of consumer choice on the Internet incentivizes companies to respond to consumer preferences, and provide them with transparency and choice regarding their use of data.

3) The Commission’s authority under Section 5 is an important piece to the privacy and data security framework, but it must be used in a responsible and principled way.

While the FTC has authority to enforce provisions of the sectoral privacy laws, it can also leverage its authority to police unfair and deceptive acts or practices (“UDAP”) to deter certain data activity. Since the Pitofsky Hearings, the FTC has used its Section 5 authority to bring actions for alleged UDAP violations for security breaches, uses of precise location data, and failures to provide adequate notice to consumers, amongst other data privacy and security practices.²⁵ We urge the Commission to pursue unfair and deceptive acts or practices focused on concrete, identifiable, and substantial consumer harms.

²⁴ *Id.*

²⁵ See e.g., *FTC v. Wyndham Worldwide Corporation et. al.*, First Amended Complaint for Injunctive and Other Equitable Relief, Case No. CV 12-1365-PHX-PGR (D. Az. Aug. 9, 2012); *US v. InMobi Pte Ltd.*, Complaint for Permanent Injunction, Civil Penalties and Other Relief, Case No. 3:16-cv-3474 (N.D. Cal Jun. 22, 2016); *FTC et. al. v. Vizio, Inc*, Complaint for Permanent Injunction and Other Equitable and Monetary Relief, Case No. 2:17-cv-00758 (Feb. 6, 2017).

In a concurring statement to the Commission’s recent Vizio case, then-Acting Chairman Maureen K. Ohlhausen questioned whether the Commission’s conclusion that television viewing information is in fact sensitive in nature, and whether sharing such information constitutes a “substantial injury.”²⁶ In that statement she further noted that the Commission cannot make a determination that an action is unfair based on only public policy, but must determine if there is substantial injury that cannot be reasonably avoidable by consumers and that is not outweighed by benefits to competition or consumers.²⁷

We agree with then-Chairman Ohlhausen. The Commission should review how it uses its Section 5 authority in privacy and data security cases. Specifically, the FTC should consider what actions it believes will cause substantial consumer injury, ground that determination in an established source of law, and focus its enforcement on those areas. This review could help avoid the types of potential overreach that led Congress to curtail its authority, and caused the Commission to publish the 1980 Policy Statement on Unfairness.²⁸

4) Predictive analytics and algorithmic tools drive innovation and connect consumers to the products and services they desire in a responsible manner.

In the advertising and marketing context, predictive analytics are used to predict a consumer’s likelihood of being interested in a product or service, to develop new and innovative products and services, to enhance the consumer experience by delivering relevant content, and to prevent fraud and provide secure transactions. While the technology has changed, the responsible collection and use of this data has occurred for more than 100 years.

Recent advances in methods of predictive analytics have greatly enhanced, but not changed fundamentally, the roles that advertising and marketing play in the U.S. economy. Technology and innovation have vastly improved the results of predictive analytics, yielding significantly greater returns for consumers who receive more tailored offers and advertisements, and for businesses that see higher returns on their marketing investments. The result is a more efficient and effective relationship between consumers and businesses.

Additionally, predictive analytics not only enhances the ability of businesses to engage and attract consumers, but also allows them to create more engaging and customized experiences that consumers enjoy and expect. The responsible use of data and analytics tools is necessary for a seamless cross-channel, cross-device experience for consumers. For example, tools that predict what video content consumers desire has fueled the growth of so-called “peak TV,”

²⁶ Maureen K. Ohlhausen, *Concurring Statement In the Matter of Vizio Inc.* (Feb. 6, 2017) https://www.ftc.gov/system/files/documents/public_statements/1070773/vizio_concurring_statement_of_chairman_ohlhausen_2-6-17.pdf.

²⁷ *Id.*

²⁸ Wash. Post, *The FTC as National Nanny* (Mar. 1, 1978), https://www.washingtonpost.com/archive/politics/1978/03/01/the-ftc-as-nationalnanny/69f778f5-8407-4df0-b0e9-7f1f8e826b3b/?utm_term=.015de8e7203d; FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980) <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

which in turn created a wealth of new video sources from which consumers can choose.²⁹ This rise in competition in the video marketplace has also forced companies to develop new methods of content delivery and compete for viewers' time by developing more engaging content.

In addition to the countless benefits that predictive analytics provide, consumers are also protected from potential misuses of such tools by bad actors. The traditional sectoral laws that prohibit discrimination, such as the FCRA and the Fair Housing Act, still apply to the use of predictive analytics and algorithms to make eligibility decisions about consumers' lives. In addition to the existing legal standards, the DAA Principles prohibit the use of web viewing and mobile app usage data for eligibility purposes related to employment, insurance, credit, and healthcare treatment.³⁰ Backed by these legal and self-regulatory restrictions on the use of data for certain purposes, either through an algorithm or other means, companies are able to innovate within a set of guardrails that allow new services for consumers while protecting them from harm.

5) Federal and state laws regarding the Internet should be consistent to allow the Internet to continue to function in a cross-border manner, free from arbitrary roadblocks.

It is important that the cross-border nature of the Internet be respected, and that any laws that apply to data collection and use on the Internet be consistent. Absent a consistent regime across the United States, a consumer in one state may experience a wholly different Internet compared to a consumer in another state. This could lead to consumer confusion, misinformation, frustration, and potentially harm and fraud.

Evidence of this experience is shown through the harm that the European Union's General Data Protection Regulation ("GDPR") has already caused the European marketplace. For example, some U.S.-based advertising companies, consulting services, and video game developers decided to exit the market, lose potential revenue, and no longer employ their European employees instead of risk potential violation of the restrictive requirements of the GDPR.³¹ Even today, months after implementation, major U.S.-based news organizations refuse to allow EU citizens and U.S. consumers abroad with access to their content, thus depriving those citizens of valuable journalistic insight into world events.³² This stands in stark contrast to the United States, where our sectoral laws and strong enforcement, coupled with industry self-regulation that promote the responsible use of data, has created the flourishing U.S.-based Internet economy that is the same from state to state. This model, however, is under threat from a patchwork of state laws.

²⁹ See e.g., Enrique Dans, Forbes, *How Analytics Has Given Netflix The Edge Over Hollywood* (May 27, 2018) <https://www.forbes.com/sites/enriquedans/2018/05/27/how-analytics-has-given-netflix-the-edge-over-hollywood/#7b3a8816b23a>.

³⁰ *MSD Principles* at 4-5; *Mobile Guidance* at 31-32.

³¹ 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>.

³² Jeff South, Nieman Lab, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after the 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/>.

The FTC should leverage the tools at its disposal to ensure that the Internet experience for consumers in the United States does not balkanize based on lines on a map. The recent passage of the California Consumer Privacy Act of 2018 threatens just that result.³³ The economic and societal benefits of the Internet would not be possible if Californians and Virginians could not collaborate on or have access to the same tools based on the same information, supported by a common and consistent legal underpinning. Additionally, bad actors could leverage different rules, platforms, and notification requirements in different states to cause consumer confusion, disseminate misinformation, or commit fraudulent activity.

In order to avoid this outcome, the FTC should partner with the other consumer protection authorities in the states, as well as industry participants, to establish consistent “rules of the road” within which the marketplace can operate. Such rules should allow for flexibility in order to foster innovative products and new data uses and tools, while protecting consumers from identifiable harms. Such cooperation is the bedrock of our federal system, and ensures that every state in the United States is able to benefit from the Internet. For example, the study commissioned by the IAB found that 86% of the ad-supported Internet economy’s direct employment and value accrue to states not traditionally considered high-tech hubs.³⁴ That study found that West Virginia’s state gross domestic product benefited from the ad-supported Internet in the amount of \$4 billion, and supported 11,792 full time jobs in that state.³⁵ If individual states create inconsistent rules, these widespread benefits may become consolidated in a small number of states. We hope that the FTC will work to ensure that consistent rules for the Internet are implemented, so as to ensure that these benefits are equally available across the nation.

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the FTC on this issue. If you have questions, please contact Michael Signorelli at 202.344.8050.

Respectfully submitted,

American Advertising Federation
American Association of Advertising Agencies
Interactive Advertising Bureau
Network Advertising Initiative

August 20, 2018

CC: Stu Ingis, Venable LLP
Rob Hartwell, Venable LLP

³³ Cal. Civ. Code § 1798.100 (effective Jan. 1, 2020).

³⁴ See *Value of Data*.

³⁵ IAB, *The Economic Impact of West Virginia’s Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/West-Virginia.pdf>.