



**Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580**

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on the

**Competition and Consumer Protection in the 21st Century Hearings, Project Number
P181201**

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
Michael Signorelli
Tara Potashnik
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

August 20, 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 “Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201” published on June 20, 2018.¹

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 service 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 Commission’s request for information regarding the promotion of competition and enforceable consumer protection is timely—in particular given recent developments in international and U.S. state law that threatens the efficiency and competition in the Internet marketplace. Some jurisdictions, such as the European Union (“EU”) and California, have taken a more restrictive approach to regulating data than the United States. This restrictive approach threatens the free flow of information and impacts U.S. consumers and businesses. We urge the FTC to set as its priority the advocacy and support for strong consumer privacy protections at a level that ensures that consumers continue to have access to the full benefits of the Internet and that fosters the United States’ leadership in the digital economy. ANA members have long supported providing consumers with transparency in data practices, privacy controls, and other privacy protections embodied in the U.S. federal regulatory framework and the self-regulatory programs that enhance those laws. Consumers also should be able to continue to reap the benefits of free and low-cost online content, products, and services through the ad-supported Internet, which the U.S. federal framework provides.

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 We anticipate that the Commission will likely observe that the Internet-based economy in the EU will suffer under the GDPR and that consumers will become frustrated due to notice fatigue. While it is too early to understand the full effects of restrictions placed on data flows like those created by the GDPR or CCPA, consumers are already experiencing the consequences of these broad, inflexible restrictions. For example, many

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>.

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).

companies elected to pull their products and services out of Europe rather than expend the significant resources required to comply with the GDPR.³ Such actions leave consumers, including U.S. consumers traveling overseas, with less choice and less access to information.⁴ Such laws may not provide the best outcome for consumers, and the FTC should study those effects to avoid unintentionally repeating them in the United States.

We first offer ANA's recommendations for consideration by the Commission. We then respond to the FTC's specific requests for comments to help the Commission guide its policy and enforcement priorities for competition and consumer protection. To that end, these comments address the following topics specifically identified by the FTC in its request: (1) the state of consumer protection law and enforcement and its development; (2) the intersection between privacy, big data, and competition; (3) the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters; (4) consumer welfare implications that may be associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics; (5) the interpretation and harmonization of state and federal statutes and regulations that prohibit unfair or deceptive acts or practices; and (6) the FTC's investigation, enforcement, and remedial processes.

I. Executive Summary: ANA's Recommendations for the Commission

We recommend that the FTC prioritize carrying out a rigorous analysis of the GDPR, the CCPA and similarly restrictive laws in order to determine their effects on competition and consumers. We also suggest that the FTC promote the U.S. sectoral model of privacy protections (alongside industry self-regulation), offer support for data-driven advertising and marketing, and advocate for industry self-regulation as part of any privacy regulatory framework. These recommendations are discussed in more detail below in the body of our comments.

A. Conduct Economic Impact Assessments of Restrictive Data Privacy Regimes

We recommend that the FTC carry out a rigorous analysis on the impact of GDPR and CCPA to determine their effects on competition and consumers.⁵ We anticipate that the Commission will find that laws like the GDPR and CCPA will limit competition, overburden consumers with opt-in notices and make an efficient and effective digital economy harder to maintain. The Commission should share its findings with legislatures and policymakers considering GDPR or CCPA-like legislation. Such research will be critical to the formulation of well-informed policy decisions and enforcement priorities. The benefits of this research are discussed in Sections II.B and III below.

³ 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>.

⁴ 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/>.

⁵ 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).

B. Promote the U.S. Sectoral Privacy Model as Opposed to Overly-Restrictive One-Size-Fits-All Privacy Standards

The U.S. federal privacy model is sectoral and targeted at concrete harms, applying detailed regulations only to specific sectors, industries, practices, or types of data where misuse of data can lead to substantial consumer harm (*e.g.*, financial data, children’s data, health data). These sectoral laws are based on the Fair Information Practice Principles. As such, the U.S. privacy model focuses on consumer protection through notice and control, based on potential harms stemming from specific types of data or its uses, rather than blanket rules that apply generally across data types and industry sectors. These sectoral laws are supplemented by industry self-regulatory principles to successfully promote the responsible online and offline collection and use of data. The Commission should incorporate this framework into any future policy approach. This framework is discussed in more detail in Sections II.A, III.B, and IV.

The EU and other jurisdictions are taking a different approach to privacy regulation, creating comprehensive one-size-fits-all privacy standards for all sectors of the economy. The rigid rules of the GDPR, for instance, impose burdensome opt-in consent requirements and restrictions on data processing that may not be reflective of consumer expectations or choice. The CCPA’s broad right to access the vast amounts of data within the CCPA’s purview create new significant avenues for identity theft and consumer fraud. The United States has historically recognized that context matters when regulating privacy. Consumers reasonably expect that companies will use information in ways that are consistent with the context in which consumers provide the data. A one-size-fits-all privacy model is not designed to recognize shifting consumer expectations and developments in technology, and will therefore stifle business practices that consumers’ value and expect, and block new entrants to the marketplace and limit competition. These threats are further discussed in Sections II.B and II.C.

C. Support Data-Driven Advertising and Marketing in the United States

The FTC should support the continued growth of the digital marketplace, and not adopt regulations that place undue burdens on it. The practice of data-driven marketing began in the United States more than a century ago, and the burgeoning data-driven marketing economy is a uniquely American creation. Just as the United States created the postal marketplace when Montgomery Ward developed the mail order catalog in 1872, so too did it create the digital marketplace by commercializing the Internet browser in the 1990s. Today, the United States leads the world in data science applied to the marketplace. Ideas developed in the United States by American statisticians and econometricians, running on U.S.-designed hardware, and coded in algorithms developed and tested in the research offices of U.S. firms, are used to generate revenues throughout the world. These contributions established the data-driven marketing industry as a major export industry – and data-driven marketing firms are a net export contributor to U.S. economic well-being. Data-driven marketing firms derive a considerable portion of their revenue abroad (sometimes upwards of 15%) while employing nearly all their workers in the United States.⁶ The FTC should support the continued growth of this industry,

⁶ Deighton and Johnson, *The Value of Data*. See summary of study, at 2, available at <http://ddminstitute.thedma.org/files/2013/10/DDMI-Summary-Analysis-Value-of-Data-Study.pdf>.

and not adopt regulations that place undue burden on it. The benefits of data-driven marketing are discussed in Sections II.A, III.B, and V.

D. Advocate for Industry Self-Regulation as Part of any Privacy Regulatory Framework

The ANA encourages the Commission to promote industry self-regulation, in addition to the sectoral privacy model that focuses on harms and respects context, as the most effective means to address privacy considerations while promoting innovation. Industry self-regulation is more flexible and adaptable than legislation, and therefore can react quickly to changes in consumer expectations or available technologies more quickly. The ability of a privacy regulatory framework to adapt to changes is especially necessary because in rapidly evolving marketplaces, context matters and consumer expectations shift over time. Self-regulation has worked for decades to help ensure responsible use of data for advertising and marketing purposes, while enabling the growth of a strong data-driven advertising and marketing economy. This model stands in clear contrast to GDPR and the CCPA. We strongly urge the FTC to prioritize policies that create strong consumer privacy protections at a level that ensures that consumers continue to have access to the full benefits of data and that maintains the United States' leadership in the digital economy, which the Commission has noted since 1996 is best served through self-regulation.⁷ The benefits of self-regulation are discussed in Sections II.A, III.A, V, VI, and VII.

II. The United States Has a Strong Record of Enforcement through Unfair or Deceptive Acts or Practices Authority, Sectoral Laws, and Self-Regulation

The United States is the global leader in the digital economy due in part to its privacy framework of sectoral laws, supported by industry self-regulation, and backed by both private and government enforcement. Below we explain how that framework functions to promote innovation, competition, consumer benefits, and respect for privacy. We then describe the unwarranted threats to this successful model by untested and overreaching frameworks. We then describe why these and other general proposals for sweeping legislation fail to strike the appropriate balance between consumer protection and economic growth and innovation.

A. The U.S. Privacy Framework Is Effective

The well-functioning U.S. privacy framework is composed of: (1) a federal regulatory scheme that is primarily sectoral and targeted; and (2) self-regulatory codes of conduct that effectively promote the responsible online and offline collection and use of data. The existing combination of sectoral laws, designed to address specific, concrete harms, complemented with enforceable self-regulatory codes of conduct, has proven to be a successful means of advancing innovation while providing consumers with transparency and control over data collection and use. We recommend that the FTC support this privacy framework in its policy development, and with legislatures and policymakers due to its ability to foster market innovation, address

⁷ 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.

consumer privacy considerations, and provide adequate protections following technological developments.

In the 1990s, the U.S. government considered comprehensive regulation of the Internet. However, it ultimately maintained the long-standing approach we have today in the United States toward privacy regulation—a sectoral framework that addresses particular areas of concern. This federal privacy model applies detailed regulations to specific sectors, industries, practices, or types of data. For example, the Health Information Portability and Accountability Act (“HIPAA”) regulates certain health data; the Fair Credit Reporting Act (“FCRA”) regulates the use of consumer data for eligibility purposes; the Children’s Online Privacy Protection Act (“COPPA”) addresses personal information collected online from children; and the Gramm–Leach–Bliley Act (“GLBA”) focuses on consumers’ financial privacy; the Equal Employment Opportunity Commission (“EEOC”) enforces a variety of anti-discrimination laws in the workplace including the Pregnancy Discrimination Act (“PDA”) and American with Disabilities Act (“ADA”); the Fair Housing Act (“FHA”) protects against discrimination in housing; and the Equal Credit Opportunity Act (“ECOA”) protects against discrimination in mortgage and other forms of lending. This harm-based approach to regulation allows consumers to reap the rewards of a data-driven marketplace while ensuring the private sector uses data responsibly to improve consumer interactions with businesses with clear limits on certain uses. This model also allows businesses to continue to innovate, by enabling the delivery of more relevant advertising, products, and services to consumers.

These sectoral laws are supplemented by industry self-regulatory principles that promote the responsible online and offline collection and use of data. For decades, the private sector has developed and enforced robust self-regulatory codes of conduct to complement the sectoral legal framework. Unlike legislation, which is static and runs the risk of codifying practices that may become out-of-date even before a bill turns into law, industry self-regulation is nimble by its very nature and thus better suited to provide protections in cutting-edge areas such as the information economy. The Commission itself recognized the value and potential of self-regulation to provide consumer protection in the realm of privacy. It stated in 1996 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” in the report that resulted from the Pitofsky Hearings.⁸ The Commission renewed this commitment in 2009 in its report on *Self-Regulatory Principles for Online Behavioral Advertising*, and saw that commitment rewarded in that space in its 2017 report on *Cross-Device Tracking* where it recognized self-regulation as improving “the level of consumer protection in the marketplace.”⁹ As the Internet ecosystem continues to evolve, the FTC should continue to back self-regulation as the appropriate model to foster innovation and support sector specific laws.

The Digital Advertising Alliance (“DAA”), an organization that the ANA helped spearhead, is a prime example of well-functioning self-regulation. DAA implemented the *Self-*

⁸ FTC, *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.

⁹ 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).

Regulatory Principles for Online Behavioral Advertising (“Principles”), a self-regulatory code that serves as a roadmap for all industry actors who collect or use data for interest-based advertising, irrespective of formal participation in the DAA program. The Principles provide consumer transparency and choice regarding data collection and use for interest-based advertising, and were drafted based on the self-regulatory practices recommended by the FTC in its 2009 report on online behavioral advertising.¹⁰

Due to self-regulation’s ability to keep pace with an evolving marketplace, the DAA has evolved its Principles as technological developments occur. For example, in 2011, the DAA extended its Principles to cover 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 to apply to uses beyond advertising.¹¹ This expansion also includes strong prohibitions on the use of such data for eligibility purposes for employment, insurance, credit, and healthcare treatment.¹² In 2013, in response to the increased use of mobile devices, DAA provided guidance on how its program addresses the collection and use of data from mobile devices, including Cross-App Data, Precise Location Data, and Personal Directory Data.¹³ In 2015, the DAA introduced guidance for the application of its transparency and choice principles to the collection and use of data across devices.¹⁴ 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 transparency and accountability to political advertising.¹⁵ Together, the Principles and subsequent guidance represent an effective framework for the collection and use of consumer data online that evolves with consumers and the ecosystem.

The main avenue through which consumers receive these disclosures and choices is through the DAA’s YourAdChoices icon.  The icon is served over a trillion times per month worldwide on websites, in apps, and in or around online advertisements delivered through interest-based advertising. The YourAdChoices icon provides transparency outside of the privacy policy, and takes consumers to easy-to-use tools to exercise choice for the future collection and use of data for interest-based advertising. These consumer choice tools are also available in Spanish in order to provide choice to even more consumers. Since the launch of the Self-Regulatory Program, participation has grown to encompass hundreds of leading companies and thousands of brands. Over 80 million visitors have now interacted with the DAA’s properties including educational pages and choice tools. In addition, consumer awareness and understanding of the program continues to increase. In a study performed in 2016, more than

¹⁰ Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009); Federal Trade Commission, *FTC Staff Report: February 2009 Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009).

¹¹ Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data* (Nov. 2011).

¹² Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data*, 4-5 (Nov. 2011); Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment*, 31-32 (Jul. 2013).

¹³ Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (Jul. 2013).

¹⁴ Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015).

¹⁵ DAA, *Digital Advertising Alliance Launches Initiative to Increase Transparency & Accountability in Political Ads*, (May 22, 2018), available at <https://digitaladvertisingalliance.org/blog-terms/political-advertising>.

three in five consumers (61%) recognized and understood what the YourAdChoices Icon represents.¹⁶

The DAA Self-Regulatory Program shows how industry can respond to the online ecosystem more efficiently than stringent government regulation. If a company fails to meet its obligations under the Self-Regulatory Program, the DAA's independent accountability programs will work to bring the company into compliance and the programs may refer unresolved matters to the FTC. The DAA accountability programs have brought more than 85 public enforcement actions since inception, underscoring the responsiveness of the program. The effectiveness of the Self-Regulatory Program also has been recognized by the United States government. In 2012, in an event at the White House, the then-Chairman of the FTC, the then-Secretary of Commerce, and Obama Administration officials publicly praised the DAA's cross-industry initiative. 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."¹⁷ The DAA's work has garnered additional praise, including from former Acting FTC Chairman Maureen Ohlhausen who stated that the DAA "is one of the great success stories in the [privacy] space."¹⁸ From 1995 to now, industry has proven the FTC correct in its assessment that self-regulation is the best path forward for digital privacy concerns.¹⁹

The *DMA Guidelines for Ethical Business Practice* ("Guidelines") are another example of longstanding and successful self-regulatory principles that provide meaningful controls and accountability to ensure that marketing data is used responsibly.²⁰ In October of 2017, DMA, now a division of the ANA, announced the release of an updated set of guidelines, including the culmination of its Data Standards 2.0 initiative.²¹ The revised standards underscore longstanding responsible data practices that: "Data collected exclusively for Marketing should be used only for Marketing purposes." In fact, the revised standards specifically prohibit the use of data for marketing in the context of eligibility determinations for employment, credit, health care treatment, and insurance, areas of primary concern where actual harm to consumers could occur. Additionally, the standards incorporate data security standards, including provisions related to contractual safeguards, data transfers, and protection of sensitive data. The Council of Better

¹⁶ 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>.

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-waitobama-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, *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.

²⁰ DMA, *Guidelines for Ethical Business Practice* (2017) available at <https://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/>. In 2018, ANA announced that it was acquiring the Data & Marketing Association (formerly the Direct Marketing Association). Press Release, ANA, ANA to Acquire DMA (May 31, 2018).

²¹ Press Release, Data & Mktg. Ass'n., *DMA Announces Final Updated Standards on Marketing Data Use, To Go Into Effect July 2018* (Oct. 10, 2017).

Business Bureaus also has a set of strong self-regulatory standards and enforcement for the ad industry and business community.

B. The U.S.-Internet Economy Is Under Unwarranted Threat

The United States created the most dynamic, competitive, and consumer friendly digital economy in the world. It did so within a well-structured and considered privacy framework of sectoral laws supported by self-regulation. Any change to that framework should be equally well-reasoned, based on sound research, and focused on addressing a concrete, identifiable, and substantial consumer harm. New laws like the CCPA, and calls to adopt an EU-like approach in the U.S., are anything but well-reasoned and calibrated to promote growth and competition while preserving consumer transparency and control over data practices.

1. These Laws Are Harmful to Competition

It is already clear that the GDPR is freezing out competition and hindering smaller, less-established, firms in the marketplace. Many American firms already left the European marketplace, removing choices from EU consumers and depriving them of the benefits of competition in an open and free marketplace.²² Additionally, by imposing costly new compliance programs, small and medium sized businesses will face serious barriers or be unable to compete with large firms that can absorb those costs. This will lead to a few winners, and many losers, in the marketplace picked in part by government regulations that were improperly vetted.

Additionally, the EU threatens to further impede the marketplace with the development of its revised e-Privacy Directive.²³ This new regulation can lead to even more restrictions on the collection and use of data online, ratcheting up requirements on companies. While e-Privacy is still being debated in Europe, reports suggest that its provisions as currently contemplated could result in an estimated loss of \$640 billion in annual revenue to entities in the Internet marketplace.²⁴ Losses of this nature will result in less competition, innovation, jobs, and benefits for consumers. Proponents of the revised Directive have identified nothing but highly speculative or ephemeral harms related to privacy as support for the need of both GDPR and e-Privacy. They clearly have not balanced whatever potential harms there may be with the very real consequences to consumer benefits and competition in the marketplace. The FTC should work to strongly advocate against any exporting of these types of broad-based, comprehensive, one-size-fits-all privacy regulations across the Atlantic.

2. These New Laws Undermine Consumer Protection

An example of this type of poorly vetted regulation that has made its way to America is the CCPA. This law surfaced and was passed in a few short days, with little to no input from

²² 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>.

²³ Natasha Singer, *N.Y. Times*, *The Next Privacy Battle in Europe Is Over This New Law* (May 27, 2018) <https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html>.

²⁴ *Id.*

stakeholders, subject to a looming deadline related to an even more onerous and senseless ballot initiative.²⁵ Among the many serious issues created by the CCPA is its extremely broad definitions of the terms “personal information” and “sale.” These terms cover vast amounts of innocuous data and activities that may only have been used to support basic business functions. The definition of “personal information,” for instance, goes far beyond definitions in current law to cover virtually 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 including non-personally identifiable information like pixel and cookie IDs.²⁶ This broad definition of personal information will mean that companies will have to collect far more information in order to effectuate the vague rights created by the CCPA, thus creating more risk of a data breach. This approach seriously undermines privacy protective activity like pseudonymization of data. The FTC supports the implementation of reasonable security measures based on the amount and sensitivity of data maintained by a company. Any new law that forces the collection of more and more detailed information from consumers for the mere purpose of complying with that law will subvert what would be considered reasonable security practices.²⁷ Further, the definition of “sale” includes renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information to another business or third party for monetary or other valuable consideration.²⁸

These amorphous definitions, and other broadly worded provisions in the law, run counter to consumers’ interests. For instance, the law includes consumer 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. The law also includes consumer opt-out rights related to the broad definitions of “personal information” and “sale” that could restrict companies from sharing personal information with certain third parties to combat consumer fraud. The law’s data deletion right, which also rests on broadly worded definitions, creates similar problems that will lead to the deletion of data used to benefit consumers. The effect of the broad and sweeping nature of the data covered by the access, opt-out, and deletion rights will only be fully realized over time, as non-sensitive data used for legitimate business functions that support the digital economy, including targeted advertising, is haphazardly deleted or blocked from being shared. Compounding these problems, the law creates a private right of action that could lead to hundreds of millions of dollars in penalties for the breach of totally innocuous non-sensitive data. All of these harms are created by the hasty process by which the state of California rewrote the settled rules for the national Internet-economy. As a result, the law will impose major costs on the public at large without providing true protection for consumers’ privacy interests.

The CCPA, as it is currently drafted, will also create new avenues for consumer harm. As the California Chamber of Commerce recent letter to the California legislature notes, the CCPA creates potential for abuses by domestic partners that may leverage its provisions to

²⁵ Janko Roettgers, *Variety*, *California’s New Privacy Law Could Have Big Impact on Tech, Media* (June 29, 2018) <https://variety.com/2018/digital/news/california-ab-375-1202861680/>.

²⁶ Cal. Civ. Code § 1798.140(o).

²⁷ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 24-26 (Mar. 2012).

²⁸ Cal. Civ. Code § 1798.140(t).

engage in stalking and other abusive behaviors.²⁹ Additionally, the drafters failed to carefully analyze the downstream effects of its newly created rights, such as criminals being able to use their right to opt-out of fraud prevention technology, or to obtain information about other consumers for use in identity theft.³⁰ Finally, some proponents of the CCPA state that compliance will be easy because large companies are complying with the GDPR, and only those large companies will be covered.³¹ This is clearly incorrect. The CCPA covers any California entity that receives personal information from only 50,000 consumers. Even the smallest companies that maintain a public website could be covered if their website records data from as little as 50,000 consumers over the course of a single year, and suffer the cost of compliance and litigation. Hundreds and thousands of small and mid-sized California companies that operate regionally and have no need to comply with GDPR may now be frozen out of the Internet economy for fear of lawsuits due to one state's decision.

3. The FTC Should Work With Stakeholders to Avoid These Adverse impacts

We need not look far for how the California law will harm the economy. The fact that GDPR-like regulations will harm the online economy has been shown in the EU already. A 2010 study by Avi Goldfarb and Catherine Tucker found that restrictions of online data use in the EU under the pre-GDPR regime lowered the effectiveness and value of advertising by 65 percent, and that general content websites like news sites were more negatively impacted by a lack of data-driven marketing.³² With the even more restrictive nature of the GDPR, these negative impacts will be amplified. As advertising becomes less effective, smaller websites will be unable to compete with established players in the EU, and competition in the online marketplace will suffer. In the U.S., many companies soon will have to comply with both the GDPR and the CCPA. The FTC should work to avoid such a result in the United States, and work with stakeholders to prevent GDPR-like regulations from taking root here.

We thus caution against the issuance of regulation, policies, or legislation such as the CCPA that could disrupt the digital economy. A patchwork of misguided regulation at the state and local level is likely to deter entry into the marketplace, thwart innovation, and limit competition. If advertising and marketing becomes less effective, it will impede companies' ability to provide online content and services to the public. This could hinder innovation or drive businesses to shift from offering free content and services to demanding direct payment from consumers, and force some market participants out if they cannot achieve a substantial paid customer base. This would substantially adversely impact consumers with limited income levels.

Given the FTC's vast expertise it has built up since the 1995 hearings related to the Internet and privacy, and its continued faith in and partnership with self-regulatory groups, the Commission should work strenuously to prevent laws, regulations, and policies based on poorly calibrated European laws or legislation forced onto a legislature at ballot-point from spreading. The FTC must now, as it has traditionally done, work with various stakeholders to provide well-

²⁹ California Chamber of Commerce et. al., *Sb 1121 (Dodd) – Business Community Requests To Be Included In Ab 375 Clean-Up Legislation* (Aug. 6, 2018) <http://src.bna.com/A44>.

³⁰ *Id.* at 11.

³¹ Common Sense Kids Action et. al, *Letter* (Aug. 13, 2018).

³² Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising* (August 5, 2010).

reasoned guidance based on research and engagement with industry to balance the need for consumer privacy and the need to continue the growth of the Internet economy in the United States that are based on the current framework that has functioned well for so long. There is no newly identifiable, substantial, consumer harm identified by proponents of these new laws that can outweigh the immense damage that upending the U.S. privacy framework would do. We should not abandon the path of targeted sectoral laws and adaptive self-regulation that the Commission has consistently endorsed.³³

C. Transparency and Control Is the Appropriate Approach to Data Privacy

The threats to the U.S.-based Internet economy and consumers' access to digital-based information and services are real and present. In addition to the issues outlined above, two other broader issues need to be kept carefully in mind regarding changing the privacy framework. The current privacy framework in the United States fosters market innovation, addresses consumer privacy considerations, and provides substantial protections following technological developments. Calls for adoption of a GDPR-like framework should be resisted, particularly given that the effects of this untested legal framework are not yet known. Careful analysis of GDPR developments will provide a strong factual foundation for further privacy proposals. For these reasons, we recommend the FTC continue to advocate for the use of the U.S. framework. Below we explain two potential approaches seen in the GDPR, CCPA, and other proposals for online privacy, and why those approaches will harm consumers and competition.

1. Opt-in Models for the Collection, Use, and Sharing of Data Are Inappropriate for Advertising Purposes

Legislative proposals that include broad opt-in consent requirements regardless of the sensitivity of the data involved are frequently put forward to address alleged privacy concerns, irrespective of any showing of actual consumer harm. These rules would create particular issues for the data ecosystem, impeding consumers' enjoyment of digital-based services while not enhancing consumer privacy.

The imposition of opt-in consent models, where companies cannot collect consumer or device data without consumers first checking a box or taking some other affirmative act, could drastically alter the digital experience. Given the collaborative architecture of the Internet, data-sharing interactions between website owners and other companies are commonly required for the orderly functioning of a website. These interactions are currently seamless, with little friction with consumers' digital experiences, and are necessary to facilitate website features and online benefits that consumer's value. A requirement for multiple opt-in consent notices will disrupt this architecture. The constant appearances of consent boxes will annoy and frustrate consumers, thereby diluting the intended purpose of such mechanisms.

³³ FTC, *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; 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).

In the online advertising industry, it has been demonstrated that the free flow and exchange of data increases the value of advertising, and helps small digital properties disproportionately in relation to established players. A 2014 study, commissioned by the DAA and carried out by Howard Beales and Jeffery Eisenach, found that availability of cookies to facilitate information transfer increases the average impression price paid by advertisers by 60 percent to 200 percent. Additionally, ads for which cookie-related information was available sold for three-to-seven times higher than ads without cookies.³⁴ The study—which focused specifically on the economic value generated by multiparty ad exchanges—also revealed that while online publishers of all sizes rely on external advertising exchanges and other third-party advertising technologies, smaller Web sites depend on them for a significantly greater portion of their advertising revenue.³⁵ The economic engine provided by data sharing and use online should not be restrained absent any identifiable and substantial consumer harm.

In the advertising and marketing world, where no record of consumer harm exists to justify a restrictive opt-in standard, we maintain that consumer privacy preferences with respect to advertising and marketing may best be expressed through implied consent or an opt-out standard with exceptions for the use and sharing of data for certain purposes. This model is the bedrock of the DAA’s self-regulatory program. Opt-in consent has not been the historical standard for digital advertising and marketing, and is not the appropriate standard for advertising and marketing going forward in any medium.

2. Vague Consumer Data Rights

Legislative proposals related to privacy often include a variety of consumer rights (*e.g.*, data access and deletion options) without assessing if consumer harm needs to be redressed. As noted earlier, consumers deserve strong Internet privacy protections at a level that ensures they continue to have access to the full benefits of the Internet. The imposition of vague consumer rights with a government imprimatur, such as the consumer rights in the CCPA and the GDPR, creates a false sense of concern in the public about the use of largely innocuous marketing data, as none of these rights are based on demonstrable harms. By extending data access and other rights regardless of marketplace injury, the State of California and the EU are implying that the collection and use of data online generally is harmful, when in fact responsible data collection and use brings significant consumer and societal benefits.

The FTC has long considered how to balance consumers’ ability to access and correct information held about them with the need for data security and to prevent identity theft and fraud. In 2005, then-FTC Chairman Deborah Majoras sent a letter to Senator Bill Nelson (D-FL) regarding proposed changes to the FCRA. In that letter, she stated that access and correction need to be carefully calibrated to prevent bad actors from “correct[ing]” data to hide it from those they are trying to defraud.”³⁶ While 13 years have passed since this letter was drafted, the fundamental facts have not. Indeed, in its 2012 report the FTC stated that the cost of providing individualized access and correction rights for marketing data would not “likely outweigh the

³⁴ J. Howard Beales & Jeffery A. Eisenach, *An Empirical Analysis Of The Value Of Information Sharing In The Market For Online Content* (Jan. 2014) <http://www.aboutads.info/resource/fullvalueinfostudy.pdf>.

³⁵ *Id.*

³⁶ Chairman Deborah Majoras, *Letter to Bill Nelson*, 4 (Jun. 14, 2005).

benefits.”³⁷ Any new consumer access, correction, or deletion rights should be centered on identifiable harms that those new rights would address, and not on vague public policy considerations.

Instead of focusing on nonexistent or speculative privacy harms, government action in the United States should focus on supporting privacy protections based on the sensitivity of data, where privacy concrete harms are more likely. The use of data for advertising and marketing allows consumers to receive information about commercial opportunities they value, and consumers are free to respond (or not) as they see fit. If a consumer does not value a particular message, the consumer will simply ignore it or opt-out. Moreover, marketing carries societal benefits as a facilitator of economic growth and competition in the marketplace, and is a form of constitutionally protected speech. Against this set of facts, it is unrealistic to suggest that vague rights of access and deletion be extended in a sweeping manner to advertising and marketing databases.

III. Data Drives Competition and Allows Companies to Provide Significant Benefits to Consumers

Data is the fuel that drives the modern, Internet-based economy. Not only does data provide companies with new and innovative means to connect to consumers, it also democratizes access to those consumers for new businesses to enter the market. Below we explain the true value of data to the U.S. economy, and then explain specifically how online advertising helps create that value.

A. The Foundational Value of Advertising and Marketing in American Society

Advertising and marketing occupies a major place in American society. Linked to the bedrock principles that shaped our nation—free speech, competition and individual choice—advertising and marketing have served the public since colonial times as a source of vital information about our open, market-based economy. Advertising and marketing serves to:

- ***Fuel economic growth.*** To compete and grow in today’s marketplace, companies must efficiently reach consumers, alerting them to new product innovations and competitive price points;
- ***Foster a wide array of affordable media choices.*** Vast, affordable media options enrich our society and underpin a core American value: the democratization of knowledge and information; and
- ***Educate the public.*** Advertising informs consumers about product choices available in the marketplace.

The goal of advertising and marketing has always been to connect consumers with the products and services they desire, when they desire them. In today’s globalizing business

³⁷ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 66 (Mar. 2012).

landscape, advertising and marketing remain foundational activities for nearly every business, helping companies provide customized offerings to an ever broader consumer audience. Advertising and marketing also generates employment and business activity throughout the economy. A recent study by IHS, a leading economic consulting firm, found that every direct job in an advertising-defined occupation (*i.e.*, those employed at advertising firms) supported 34 other jobs across a broad range of industries throughout the U.S. economy.³⁸ In addition, every million dollars spent on advertising supported 67 American jobs.³⁹

As more and more products and services move online and as consumers increasingly spend time engaging with content on digital platforms, online advertising and marketing will continue its skyrocketing growth path, as will the value that society derives from data-driven advertising and marketing practices. The Commission, and the economy as a whole, would benefit from the FTC studying the increasing value of data-driven advertising to the U.S. economy and supplementing the existing work on the topic.

B. Benefits of Online Advertising and Marketing to the Digital Economy

Advertising and marketing fuels the digital economy. Every day consumers' lives are enriched by data-driven resources, including an unprecedented array of high-quality information and entertainment. Revenues from online advertising 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.

Consumers value these ad-supported services and products and benefit from the diversity of companies online. In a recent Zogby survey, commissioned by the DAA, over 90% of consumers stated that free content was important to the overall value of the Internet, and 75% noted that they prefer content to remain free and supported by advertising rather than pay for ad-free content.⁴⁰ Eighty-five percent of consumers surveyed stated they prefer the existing ad-supported model, and 75% also indicated they would greatly decrease their online engagement if the ad-supported Internet were to go away. This same survey found that consumers value the ad-supported content and services at almost \$1,200 a year.⁴¹

As the data suggests, the current digital economy relies heavily on advertising and marketing to provide consumers the products and services they desire. A study commissioned by the Interactive Advertising Bureau ("IAB"), and 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 U.S. in 2016.⁴² Increasingly,

³⁸ IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (2015).

³⁹ *Id.*

⁴⁰ Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016), available at http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf.

⁴¹ Digital Advertising Alliance, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid*, PR Newswire (May 11, 2016), available at <http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html>.

⁴² IAB, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), available at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

however, the digital economy faces legislative threats and overly prescriptive proposals to regulate the collection and use of data, such as the recently enacted CCPA and the EU's GDPR.⁴³ To ensure that consumers continue to enjoy the online content, products, and services they receive at little to no cost to them, the data that underpins advertising and marketing must continue to be available and reactionary overly-restrictive regulatory efforts should be rejected. Strong consumer privacy protections are important and must be balanced with the other benefits of the digital economy that consumers value and expect, including personalized services, seamless product and service offerings, and affordable choices.

Data-driven marketing is also essential to the success of start-up companies that drive innovation and frequently rely on advertising revenue to establish and grow their organizations. Free flowing data enables small and innovative businesses to compete effectively with big players. The responsible use of data gives all companies, and especially small businesses, the ability to effectively and responsibly match products to customers both online and offline, thereby lowering barriers to market entry for specialized or niche offerings that previously could not have succeeded.

The imposition of rigid legal frameworks fails to account properly for both existing and future technology. This inhibits companies' ability to innovate, entrenches the existing marketplace freezing out new entrants and competition, and leaves consumers with fewer options for the products and services they desire. We urge the Commission to continue to support and promote the more flexible approach in effect in the United States.

IV. The FTC Should Focus Its Enforcement Efforts on Concrete Harms to Consumers

The U.S. framework combines specific legal restrictions, focusing on misuse of data that can cause identifiable harms, with enforceable industry self-regulation that nimbly responds to an ever-changing marketplace. This harm-based regulatory approach allows the private sector to use data responsibly and to enable the delivery of more relevant marketing. This activity provides efficiencies for consumers and boosting the economy in the process. These sectoral laws are supplemented by industry self-regulatory standards and active enforcement. This combination of strong consumer protections by the FTC, specific privacy laws, and robust enforceable industry self-regulation has proven to be a successful means of advancing innovation, while also providing consumers with immediate resolution of their concerns. It is this agile, flexible framework of protections that has helped drive innovation through responsible data practices and fuels the U.S. economy. This focus on concrete, identifiable, consumer harm should remain the centerpiece of the Commission's enforcement activities.

In 2017, then Acting FTC Chairman Maureen Ohlhausen emphasized that the FTC should focus on actual harm to consumers, consistent with the agency's statutory mandate, stating on one occasion that:

⁴³ 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).

The FTC should focus enforcement on matters where consumers are actually injured or likely to be injured, or where companies don't keep their promises, to the consumer's detriment. The agency should focus on cases with objective, concrete harms such as monetary injury and unwarranted health and safety risks. The agency should not focus on speculative injury, or on subjective types of harm.⁴⁴

Then-Acting Chairman Ohlhausen also emphasized this need for focus in her concurrence in the FTC's settlement with Vizio, Inc.⁴⁵ In that statement she emphasized that the Commission 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.⁴⁶

With regard to advertising and marketing, the Commission itself noted that the only "harm" consumers might experience from inaccurate marketing data being obtained is to receive irrelevant advertisements. In fact, additional requirements for marketing data to address harms that have not materialized would actually require the collection of more personally identifiable information to supplement marketing databases in order to increase accuracy and permit authentication of individuals who request access or changes to records.⁴⁷ This acknowledgement makes clear that use of data that could lead to inaccurate marketing decisions should not rise to the level of "substantial consumer harm."

Instead of giving credence to speculative harms that could possibly arise from the collection and use of data, which could result in potentially restrictive new policies, the FTC's focus should be addressing concrete harms that actually result from the misuse or unauthorized use of data. This focus will continue to foster the proven economic benefits that data-driven marketing provides, while protecting consumers from actual harm. ANA encourages the FTC to see the value in the U.S. tradition of focusing on discernible, concrete harms to consumers, and to exercise caution in considering any new restrictions or actions that may result in the free flow of data that could impact the United States' well-functioning and data-driven economy.

V. The Use of Algorithms, Artificial Intelligence, Big Data, and Predictive Analytics Provides Significant Benefits to Consumers, and Is Subject to Restrictions on the Use of such tools for Certain Eligibility Purposes and to Help Prevent Discrimination

Predictive analytics can help turn raw data into useful information used to prevent fraud and promote increased consumer safety. The use of predictive analytics in marketing has one purpose: to improve the likelihood that consumers receive marketing, content, and other services tailored to their interests and preferences. The results are beneficial—the delivery of a marketing

⁴⁴ Acting Chairman Maureen Ohlhausen, FTC, Opening Keynote, ABA 2017 Consumer Protection Conference (Feb. 2, 2017), https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf.

⁴⁵ 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.

⁴⁶ *Id.*

⁴⁷ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 29 (March 2012).

offer that has a greater chance of being relevant and interesting to a consumer. The innovative application of marketing analytics to big data provide benefits to society by making it more likely that an offer will be valuable to the consumer who receives it.

For example, a retailer might look at what a customer has purchased at a particular store, through its website, and from its mobile site, and then analyze those purchases in comparison to others who have bought those items. Using analytics, the retailer will predict whether a customer is more likely to want a coupon for jewelry or for kitchen appliances and use the same data to identify and improve the channels where consumers are more likely to purchase and engage with the retailer's products. When successful, these techniques give consumers more information as they navigate the commercial marketplace and help consumers to obtain the goods and services they desire at competitive prices.

The use of these innovative analytics techniques are subject to the same restrictions on the use of data for eligibility purposes as more traditional data tools. The current U.S. regulatory framework provides protections for consumers in particular areas where the nature of the data, if misused or misappropriated, could cause discernible harm to consumers. For example, FCRA protects against the use of consumer data for eligibility purposes; the Equal Employment Opportunity Commission ("EEOC") enforces a variety of anti-discrimination laws in the workplace including the Pregnancy Discrimination Act ("PDA") and the Americans with Disabilities Act ("ADA"); the Fair Housing Act ("FHA") protects against discrimination in housing; and the Equal Credit Opportunity Act ("ECOA") protects against discrimination in mortgage and other forms of lending using traditional method or new big data enabled predictive analytics. In these contexts, the law imposes obligations on the user of the information, such as notifying the consumer of an adverse decision and providing other information relating to the use of a credit report in making the decision. In addition to these federal laws, the DAA's *Self-Regulatory Principles* prohibit the collection, use, or transfer of web viewing and mobile app usage data for employment eligibility, credit eligibility, health care treatment eligibility, and insurance eligibility, including underwriting and pricing. These restrictions are backed by the DAA's accountability programs (discussed further below in Section VII). The use of predictive analytics in marketing has no such adverse impact. Marketers use predictive analytics to reach out to groups of consumers to advertise, offer, and otherwise deliver content.

Even when predictive analytics are used to determine potential discounts or prices for goods, this does not rise to the level of "price discrimination." On a basic level, price differences occur in the marketplace for many reasons, including the costs associated with delivering products to different locales (*i.e.*, the placement of distribution centers relative to the consumer seeking to purchase a good). However, in many instances, predictive analytics have the effect of lowering prices for consumers and increasing the quality of customer service. This is no different than the price or service differences between consumers that result when one consumer is part of a customer loyalty program and the other is not. Frequent flyer programs serve as a good example. Frequent flyer members often receive preferred services such as early boarding privileges, access to airport clubs, and specially tailored flight offers. At the same time, new customers may receive a coupon or better pricing than current customers in an attempt by the business to acquire new customers. Consumers do not label such discounts pejoratively as causing "disparate impact" or establishing "price differentiation schemes" because these

discounts lower prices for consumers and increase the quality of customer service. Similarly, marketing tools that help match consumers with relevant offers do not harm the public, but in fact benefit consumers through greater efficiency and lower costs. The FTC has adequate power under false, deceptive or unfair acts or practices authority, to stop any programs that could harm consumers in this area.

This framework has allowed the private sector to use data responsibly to improve consumer interactions with businesses with clear limits on certain uses, while at the same time enabling the delivery of more relevant marketing through the use of big data and evolving analytical models and tool.

VI. State and Federal Laws Prohibiting Unfair or Deceptive Acts or Practices Should Be Enforced Consistently across the United States

Consistency across the United States with respect to laws prohibiting unfair and deceptive acts and practices is a critical factor for providing consumer protections alongside a competitive innovation-friendly market. Consistency among states and the federal government provides companies with the certainty they require to develop and offer new products and services to consumers. As seen with the passage of the CCPA, a patchwork of state laws could soon emerge and fracture the existing marketplace. ANA urges the FTC to continue to work with stakeholders at the federal and state level to harmonize enforcement, and to provide businesses with clear direction on regulators' expectations and interpretations of the law. For example, the FTC has continued to advance the EU-US Privacy Shield, most recently settling claims with a company for misrepresenting its compliance with that framework.⁴⁸ The FTC's enforcement role in this context is important to the continued viability of the free flow of information across borders to facilitate the economic growth of the Internet-enabled economy.

Outliers with respect to the laws themselves or enforcement create uncertainty with respect to applicable standards. An uncertain regulatory environment leads businesses to scale back their operations—creating fewer economic and commercial opportunities for consumers. As we noted above, the FTC should scrutinize new, burdensome requirements as they may limit economic growth while not effectively enhancing consumer protections.

VII. Enforcement of Self-Regulatory Programs Provides a Critical Supplement to the Commission's Investigation, Enforcement, and Remedial Processes

As it has done for more than twenty years, the FTC should continue to support the accountability programs that enforce self-regulatory codes as a valuable supplement to the Commission's own enforcement efforts. For example, the DAA's *Self-Regulatory Principles* are subject to strong enforcement through its accountability programs. If a company fails to meet its obligations under the DAA's Self-Regulatory Program, the DAA's independent accountability programs will step in to enforce against violations. For uncorrected violations, the

⁴⁸ *In re ReadyTech Corporation*, Agreement Containing Consent Order, No. 1823100 (Jul. 2, 2018) https://www.ftc.gov/system/files/documents/cases/1823100_readytech_consent_7-2-18.pdf.

Accountability Programs may report these cases to the appropriate government agencies.⁴⁹ These self-regulatory programs supplement the FTC's strained enforcement resources by monitoring the market for compliance, and correcting bad behavior.

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.⁵⁰ The work by the DAA's accountability program has improved compliance with those principles across the marketplace, and increases the level of consumer protection on the Internet in a way that the FTC is unable to do alone. The DAA's program has been recognized by the FTC itself as a program with "teeth."⁵¹

As another example, the DMA Guidelines have been enforced against companies for decades. Such enforcement of the Guidelines has occurred in hundreds of data-driven marketing cases concerning deception, unfair business practices, personal information protection, and other practices that could result in injury to consumers. Most companies work to voluntarily cease or change the questioned practices. However, if a company declines to cooperate and a violation of the Guidelines has not been resolved, the matter can be made public and referred to the appropriate regulatory agency including the FTC.

By continuing to work with industry self-regulatory bodies, the FTC can expand its ability to protect consumers and provide clear guidance to companies regarding responsible and appropriate data collection, use, and transfer online.

* * *

The ANA appreciates this opportunity to comment on the appropriate 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 Commission on these issues.

⁴⁹ Which has occurred once in the history of the DAA's Accountability Programs. Council of Better Business Bureaus, *SunTrust Bank Referred to the CFPB for Refusal to Participate in Self-Regulation* (May 2014).

⁵⁰ *Id.*

⁵¹ Remarks of FTC Chairman Jon Leibowitz at White House Privacy Event (Feb. 23, 2012) <http://www.ftc.gov/speeches/leibowitz/120223whitehouse-privacy.pdf>.