Developing the Administration's Approach to Consumer Privacy

comments of the

Network Advertising Initiative (NAI)

filed with the

National Telecommunications and Information Administration

November 9, 2018

I. Introduction

Thank you for providing this thoughtful, comprehensive approach to enhancing consumer privacy and balancing the need to promote robust innovation, and for the opportunity to comment. The NAI concurs that privacy protections should be principles-based and focus on outcomes and benefits to consumers, rather than seeking to enshrine complex consent procedures or prescriptive interface designs in law.

The NAI recognizes two key goals a national privacy law should seek to accomplish. First, it must provide adequate privacy protections for consumers' personal information. Those protections should include a right to be free from harmful and unreasonable data practices. Second, it must promote our thriving Internet and information-driven economy, where robust innovation drives strong economic growth, employing millions of Americans and providing transformative benefits for consumers.

We believe that these goals are not mutually exclusive, and we offer the following detailed comments to help advance this discussion. We look forward to engaging with the Administration and Congress in support of a national privacy law regarding the collection and use of consumer data. In summary, these comments offer the following key points:

- The NAI is the leading self-regulatory organization for digital third-party advertising, requiring member adherence to a strict code of conduct.
- The ad-supported Internet ecosystem has proven essential and highly desirable for consumers, businesses, and the economy.
- The current state of policy fragmentation is an impediment to cutting-edge innovation, and it will likely be exacerbated in the absence of a national privacy framework in the United States.
- Consumers, U.S. companies, and the overall U.S. economy would benefit substantially from a sensible, uniform federal law that builds on our current regime and leverages self-regulatory efforts.
- The NAI Code of Conduct is FIPPs-based and outcomes oriented, and we believe this type of self-regulation should be a critical component of a national framework that protects privacy and encourages innovation.
- An effective national privacy framework must continue to incentivize data minimization, pseudonymization, de-identification, and other privacy protective practices.
- A national privacy law should seek to correct shortcomings created by existing models, such as the GDPR and CCPA, including:
    - Provide for responsible data stewardship by all entities in the ecosystem, rather than favoring first or third-parties;
    - Clarify individual control rights, which can create substantial challenges for authentication within the third-party advertising industry, and if not done effectively, could potentially lead to the collection of *more* personal information;

    - Allow publishers and service providers to charge a fee as an alternative to using a free advertising supported model.
- The FTC is well suited to remain the primary regulator of consumer privacy, but a national privacy law should provide greater clarity around enforcement of unreasonable data practices and increased resources for FTC enforcement.

II. The NAI is the leading self-regulatory organization for digital third-party advertising, requiring member adherence to a strict code of conduct.

The NAI is a non-profit organization that, since 2000, has been the leading self-regulatory organization dedicated to responsible data collection and use governing third parties engaged in personalized advertising and ad delivery and reporting (ADR) in the United States.

The NAI has over 100 member companies, each of which is required to adhere to the strong digital advertising best practices set forth in the NAI Code of Conduct by implementing stringent consumer privacy protections. The NAI employs a variety of means to verify that its members adhere to the privacy commitments embodied in the NAI Code. In the event a compliance deficiency identified by any of these means remains unaddressed by a member, the NAI also retains the power to impose a range of sanctions, including referral to the FTC and suspension or revocation of NAI membership. At the same time, by requiring all members to publicly attest to compliance, the NAI Code provides a basis for FTC enforcement in the event of non-compliance.

Our members include a wide range of businesses such as ad networks, exchanges, platforms, and other technology providers.[1] Across websites and mobile applications, our member companies form the backbone of the digital advertising ecosystem – helping advertisers reach audiences most likely to be interested in their products and services while allowing consumers to receive ads that are personalized to their interests.

The NAI Code and associated guidance continually evolves to adapt to changes in technology and consumer expectations. For example, the NAI issued guidance this year to address how our members may and may not collect and use information about the video content consumers view on a television for the purposes of personalized advertising, helping to ensure that consumers are provided with notice and choice with regard to data collection in this developing area where consumer expectations and understanding may be lagging behind innovation. In addition, the NAI is currently undertaking a major update to the Code that will include robust new privacy protections. The NAI expects to introduce the new Code in 2019. The rapid changes in technology to which the Code applies, as well as the requirement that our members provide consumers with a choice regarding how those technologies collect and use information about them, requires an ongoing effort by the NAI to adapt. This is evident

[1] NAI membership spans various technology platforms, including demand side platforms (DSPs), supply side platforms (SSPs), data management platforms (DMPs) and audience management platforms (AMPs).

from the fact that the NAI has already published three updates to the Code and four guidance documents since 2012, in order to keep up with the rapidly evolving digital advertising ecosystem.

III. The ad-supported Internet ecosystem has proven essential and highly desirable for consumers, businesses, and the economy.

Today, a broad array of rich content is available on the Internet, including information and news content, video and music streaming services, and interactive software services such as email and social networks. These have all experienced robust growth over the last several years, providing a wide array of transformative benefits to consumers for free, or for little cost, supported by digital advertising. Digital advertising, particularly personalized advertising, has been the lifeblood for the Internet and the digital economy, providing significant benefits to consumers by connecting them with products and services that are more relevant to their interests, and providing opportunities for American businesses large and small to connect with consumers. A federal privacy law is the only way to achieve NTIA's goals of harmonizing privacy regulation and establishing a consistent privacy framework for both consumers and companies.

As the Internet-based media ecosystem has become richer and more diverse over nearly three decades, one thing has remained constant: by far the most popular model among consumers is free or low-cost ad-supported content. This conclusion is supported by significant research that measures the value consumers place on ad-supported content. Notably, recent data from Nielsen suggests that while the media landscape expands, the type of content consumers are spending time with has remained fairly consistent. Ad-supported content remains the medium that consumers gravitate toward the majority of the time in their viewing habits.[2] According to Nielsen data, the share of time spent with ad-supported content on platforms (such as TV, radio, smartphones, video games and tablets) for adults in 2017 was 86%—a number that has remained relatively flat over the past decade.[3] Nielsen's broad conclusion based on this research is as follows:

> *Although consumption of ad-supported media has varied over the past 15 years, it is still far more dominant and successful than perception may indicate. Today, ad-supported content remains a consumption stalwart as consumers' media palates expand and consumption habits swell. While such revenue models have existed for some time, they seemingly have the versatility and adaptability to keep pace with an ultimately dynamic and fragmented landscape. This new age of media consumption allows marketers and advertisers to reach consumers in more ways than ever before and do so with ease.*[4]

The NAI recently conducted a consumer survey that produced similar results. In late 2017, we ran opinion polls and marketing research on Internet users through a survey that obtained responses from 10,000 U.S. consumers to assess their opinions on privacy, digital advertising, and the ad-supported

[2] Nielsen Company, *As the Media Universe Grows, Ad-Supported Content Remains a Preferred Source* (March 14, 2018).
[3] Ibid.
[4] Ibid.

Internet. The survey revealed that respondents overwhelmingly prefered their online content to be paid for by advertising, at a rate of 67%, a result that was substantially consistent across all age-groups.[5]

While it is hard to measure the overall value that advertising-based content provides to consumers, a survey commissioned by the Digital Advertising Alliance (DAA) revealed that consumers valued ad-supported services like news, weather, video content, and social media at $99.77 per month, or $1,197 per year. 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.[6]

Other research has explored the value of different types of advertising. An economic study by Professor Howard Beales and Jeffrey Eisenach of Navigant Economics found that the use of cookie technology to increase relevance of advertising increased the average impression price paid by advertisers by 60% to 200%, depending on a series of variables.[7] This data underscores the value of personalized advertising, whereby data used to determine the relevance of ads is a critical variable for successful ad-supported content. When advertisers are willing to pay more for impressions, consumers are able to enjoy a wider range of free or low-cost web content, mobile applications, and other services. Typically, this results in an improved user experience by decreasing the total number of ads displayed. This is particularly true for smaller publishers and app developers who would not otherwise be able to attain sufficient revenue to serve their consumers.

Research also demonstrates the considerable economic contribution provided by digital advertising. A 2017 study by Harvard Business School Professor John Deighton found that the U.S. ad-supported Internet created 10.4 million jobs in 2016. This research concluded that 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.[8]

IV. The current state of policy fragmentation is an impediment to cutting-edge innovation, and it will likely be exacerbated in the absence of a national privacy framework in the United States.

Over the last several years, and particularly with the recent implementation of the General Data Protection Regulation (GDPR) and the enactment of the California Consumer Privacy Act (CCPA), the Internet ecosystem is threatened by a fragmentation of policies governing consumer data collection and use. This fragmentation is likely to have many unintended consequences that conflict with the objectives of the underlying policies. These consequences include confusion among consumers about privacy expectations; threats to innovative Internet-based services and applications that rely on data

[5] Digital advertising, online content, and privacy survey, Network Advertising Initiative (April 9, 2018).
[6] Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet, Commissioned by the Digital Advertising Alliance (May 2016).
[7] Beales, Howard , and Eisenach, Jeffrey, *An Emperical Analysis of the Value of Information Sharing in the Market for Online Content*, commissioned by the Digital Advertising Alliance (January 2014).
[8] Deighton, John, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017).

collection and use; degraded user experiences for consumers; and a regulatory environment where companies struggle to comply with a patchwork of requirements around consumer data that are both stringent and inconsistent with one another.

Since the GDPR went into effect in May, companies have spent billions of dollars assessing and implementing compliance. Research reveals that large companies led the way with compliance, with the cost to Fortune 500 companies estimated to be $7.8 billion in May 2018, or an average of $16 million per company.[9] Compliance costs were a major contributor to some U.S. sites going dark in Europe following implementation.[10] In many other cases, user experiences have been substantially degraded by redundant requests for consent. Additional research has recently found post-GDPR effects on EU ventures, relative to their US counterparts. The negative effects manifest in the overall dollar amounts raised across funding deals, the number of deals, and the dollar amount raised per individual deal.[11]

GDPR has indeed led to an environment where businesses are limited in their ability to provide a personal user experience for their visitors and customers, and it has also led to a spike in marketing emails from companies asking their subscribers to provide permission to keep them on their mailing lists.[12] Although it is hard to draw firm conclusions within only six months, the GDPR is likely to lead to decreased choices for consumers and limit economic growth.

Additionally, there are widespread concerns that the challenges smaller companies face when attempting to comply with prescriptive regimes such as GDPR and CCPA will entrench larger, established companies in their current market position, creating a barrier to market entry for many small and mid-sized companies that ensure continued innovation and competition with bigger players. FTC Commissioner Noah Phillips recently expressed this concern, noting, "laws and regulations intended to promote privacy may build protective moats around large companies (some of which already possess significant amounts of data about people) by making it more difficult for smaller companies to grow, for new companies to enter the market, and for innovation to occur—and insist that competition be part of our conversation about privacy."[13]

U.S. Department of Justice Antitrust Division lead, Makan Delrahim, has made a similar point, noting that the costs of regulatory compliance will "create entry barriers" that incumbents might be willing to incur "if the same cost is applied to new competitors."[14] Adam Thierer also recently concluded that if

---

[9] Smith, Oliver, Forbes, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown* (May 15, 2018).
[10] South, Jeff, Nieman Lab, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after the GDPR took effect* (August 7, 2018).
[11] Jia, Jian and Jin, Ginger Zhe and Wagman, Liad, The Short-Run Effects of GDPR on Technology Venture Investment (November 5, 2018), available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912&download=yes
[12] Spilka, Dmytro, Business 2 Community, *How GDPR Can Undermine Personalization and User Experience* (August 15, 2018).
[13] Phillips, Noah, *Keep It: Maintaining Competition in the Privacy Debate* (July 27, 2018).
[14] Assistant Attorney General Makan Delrahim Delivers Keynote Address at the University of Chicago's Antitrust and Competition Conference (April 19, 2018), available at: https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-keynote-address-university-chicagos

new regulations aimed at requiring existing tech platforms to adopt stronger privacy practices are imposed on all companies indiscriminately, those regulations would likely "end up hurting smaller rivals more and create barriers to new entry and innovation going forward."[15]

Recent enactment of the CCPA, which will become operative on or before July 1, 2020, now requires the same companies to spend many more months and billions of additional dollars to perform further legal and data flow analysis and implementing procedures to comply. Despite the lack of clear regulatory guidance from the California Attorney General, analysis of the law and contrasts between the policies reveals that compliance with one will not translate effectively into compliance with the other. While both the GDPR and CCPA establish a set of qualified and enhanced rights for consumers, both also place less emphasis on promoting innovation, they both suffer from some flaws in drafting, and both are substantially ambiguous with respect to implementation, which contributes significantly to compliance costs.

In addition to California's activity around CCPA, additional states are expected to consider adopting new privacy regulations that will likely result in additional conflicts with CCPA, GDPR, and existing privacy laws in the U.S. The patchwork of state privacy laws proliferating in the United States is not a desirable outcome for consumers, businesses, or regulators, and will inevitably raise compliance costs for businesses.

V. Consumers, U.S. companies, and the overall U.S. economy would benefit substantially from a sensible, uniform U.S. federal law that builds on our current regime and leverages self-regulatory efforts.

The NAI does not believe any of the points above are arguments against needed privacy protections. Rather, we support the adoption of a new federal privacy law that reduces the complexity of compliance through preemption of state privacy laws, which inevitably will become conflicting. The NAI urges policymakers to be mindful that any new privacy regulations will come with additional costs, and to ensure that any consumer privacy gains that may result from new regulations are commensurate with these additional costs to businesses and consumers, including the competitive harms that may result from increasing the costs of market entry, and increased direct costs to consumers if regulations limit the use of personalized advertising.

There is growing consensus that consumers, U.S. companies, and the overall U.S. economy would benefit from a uniform federal privacy law that promotes consumer privacy and provides protection from unreasonable data practices that could result in consumer harm. Such a law would both serve as a vehicle to avoid regulatory fragmentation and improve on the shortcomings of existing models like the GDPR and CCPA.

[15] Thierer, Adam, *The Week Facebook Became a Regulated Monopoly (and Achieved Its Greatest Victory in the Process)* (April 10, 2015).

A new federal privacy law should establish a uniform framework that presumptively applies to all companies, but it also could retain existing federal privacy laws that have for many years provided an effective framework for protecting Americans' sensitive information, including financial, health, eligibility, and children's data. This risk-based regime appropriately targets concrete, specific harms that can arise from the misuse of information in cases where sensitivity and privacy risks are heightened.

While a federal privacy law in the United States would not be a panacea for global fragmentation, it could nonetheless be effective in providing a consistent set of protections for U.S. consumers and setting clear expectations for businesses. While NAI does not believe the GDPR is an appropriate model for U.S. privacy regulation, a timely U.S. privacy framework has the potential to maximize interoperability and minimize compliance conflicts with the GDPR. Such a framework would also provide the United States the opportunity to lead internationally by providing an alternative model to the GDPR as many other nations look to develop their own privacy laws.

VI. The NAI Code is FIPPs-based and outcomes oriented, and we believe this type of self-regulation should be a critical component of a national framework that protects privacy and encourages innovation.

Self-regulation remains uniquely positioned to promote innovative approaches to consumer transparency and choice in a dynamic technology marketplace. There are myriad different types of data collection across a wide range of platforms, services and devices, which continue to grow with the development of the Internet of Things. Given this market reality, there would be several concrete benefits to including self-regulatory organizations as part of the enforcement paradigm for federal privacy legislation, including: to leverage the existing industry expertise and experience that is housed in long-standing SROs; to extend the reach of enforcement efforts without requiring the commitment of additional public resources; and to promote consumer privacy by providing regulators with additional tools through which any new privacy requirements may be monitored and enforced.

The NAI Code of Conduct governs the way our members collect and use data for personalized advertising, and it is a premier example of a compliance framework that can be leveraged by a new federal law. The NAI developed its Code, which we continue to revise and update, through consultation with both industry and non-industry stakeholders, including the FTC and privacy advocates. The NAI Code is rooted in the nearly universally accepted FIPPs, and it applies those principles so that when our members engage in personalized advertising, they must meet strict obligations with respect to transparency and purpose specification, user control, data minimization, use limitation, data quality and integrity, security, as well as accountability and auditing.

Our robust self-regulatory program can serve as a model for how government regulation and industry self-regulation can combine to encourage broad compliance across a large and diverse ecosystem for data collection and use. We urge Congress and the Administration to include a presumption of compliance for companies that adhere to strictly aligned self-regulatory codes, such as the use of a safe

harbor model to combine government regulation with self-regulatory efforts. The Children's Online Privacy Protection Act (COPPA) took this approach to promote broader compliance.

The COPPA safe harbor program, which has proven effective for two decades, employs FTC-approved industry self-regulation bodies to administer compliance programs. These compliance programs have several important benefits. First, they streamline FTC enforcement efforts and allow the Commission to focus its limited resources on bad actors, instead of those companies working with safe harbors to comply with COPPA. Second, safe harbors incentivize companies to invest time and resources into compliance. Finally, these positive results are achieved with far fewer public resources than would be required if FTC administered the safe harbor program on its own. To date, the Commission has brought more than 20 enforcement actions under COPPA, while safe harbor programs have worked non-stop to promote and ensure compliance for hundreds of companies.

VII. An effective national privacy framework must continue to incentivize data minimization, pseudonymization, de-identification, and other privacy protective practices.

As the RFI notes, effective privacy protections rely on the definitions of key terms. This begins with meaningful definitions of "personal information" (PI) and "sensitive information." It is critical for a privacy framework to encourage companies to embrace privacy-protective practices that are tailored to the level of sensitivity of the data those companies are processing, rather than lumping all types of data together with broad definitions. Broad definitions remove incentives for data de-identification, pseudonymization, and minimization. For example, any federal privacy law should deter companies from collecting or using information like full names, email addresses, and phone numbers when they can accomplish the same business goals by using pseudonymous identifiers.

One of the most important elements of the NAI Code is the incentive it creates for NAI members to avoid collecting personal information, and to ensure that any personal information they process is not used for purposes of personalized advertising. Under the Code, pseudonymous identifiers are particularly important for privacy protection because they allow companies to recognize a browser or device without collecting any information that directly reveals the identity of the individual using that device.

The NAI does not contend that such identifiers (such as device IDs, browser IDs, or IP addresses) may not technically be linkable to PI given adequate time and resources. Our position is simply that those identifiers actually enhance privacy for consumers when companies do not link them to PI in practice. All NAI members have committed to providing consumers with a choice before any information used for personalized advertising (such as marketing or interest segments associated with a browser ID) is linked with PI. Combined with appropriate administrative controls that prevent inadvertent linking of such information to PI, this provides for a privacy protective environment.

The CCPA provides an example of how PI can be defined in a way that actually disincentives companies to continue using pseudonymous identifiers in lieu of names, email addresses, etc. The CCPA, as

currently drafted, uses an expansive definition of PI that encompasses pseudonymous identifiers as well as traditional PI. Because companies face the same compliance obligations under CCPA with respect to both pseudonymous identifiers and PI, they have no incentive to go through the work of creating pseudonymous identifiers. As such, CCPA robs consumers of the actual privacy benefits pseudonymous identifiers provide in favor of protecting against the hypothetical risk that companies could associate those identifiers with PI, even if companies never do so in practice. A new federal privacy law should avoid this mistake.

Any effective privacy law or regulation, particularly a new federal law, must recognize and take into consideration the privacy-promoting value of using pseudonymous and de-identified data when combined with appropriate administrative controls, such as appropriate notice and choice for consumers, before attaching such data to an identified person.

The definition of "sensitive information" is also a critical element in promoting privacy for consumers. Both the GDPR and the CCPA have adopted an overly-broad definition of sensitive information, and this is one of the areas where a national privacy framework could benefit from a more thoughtful, flexible approach. In further assessing what types of information it considers to be "sensitive," a national privacy law should recognize that expectations of privacy are not uniform across consumers, and they evolve over time. An effective framework that can evolve with technology and consumer expectations should refrain from drawing conclusions that are likely to become outdated and inconsistent in a matter of months or years.

These and other critical definitions represent key areas where the NTIA could help to inform this discussion through further deliberation with leading experts and key stakeholders.

VIII. A national privacy law should seek to correct shortcomings created by existing models, such as the GDPR and CCPA.

1. Provide for responsible data stewardship by all entities in the ecosystem, rather than favoring first or third-parties.

In crafting a national privacy framework, it is critical to recognize that both first party and third-party service providers play different, but often complementary, roles for consumers in the Internet economy—this is true in both online and offline environments. While there are different types of first-party and third-party companies, the key distinction is that first parties are the entities that consumers deal with directly, and third parties are the entities that do not have a direct relationship with the consumer, and instead generally provide services to first parties. For example, a news website that connects directly with consumers via account creation is generally a first party, while a company that provides insights about users of that news website through web analytics and personalized advertising services is generally a third party. In different circumstances, the same company may be either a first party or a third party.

The fact that a company collects information about consumers in a first-party instead of a third-party context does not make that company inherently better at protecting consumer privacy. For example, a sophisticated third-party web analytics company may have much greater experience and technical ability with consumer privacy and security than a small first-party blog that collects registration information from users. Therefore, a federal privacy law should apply equally and promote good data stewardship among both first and third-parties, and hold accountable companies that do not meet their obligations, regardless of where they sit.

Instead of focusing on first vs. third party relationships, a national privacy framework should focus on what type of data each entity collects, the purpose for which they were collected, the sensitivity of the data, and how the data are used and secured. Transparency around data sharing is critically important in any case, but seeking to broadly limit data sharing among first and third parties would lead to a false sense of privacy and security for consumers, who could suffer equal harm from bad data stewardship by first-parties who do not share data with a third party. For instance, the CCPA places an unnecessary and unhelpful emphasis on data sharing, rather than collection and use, likely creating an unfounded fear around sharing with responsible third parties. In fact, responsible data sharing is essential to promoting the growth and development of new technologies like machine learning, unlocking new insights through data analytics, and making ad-supported content and services widely available to consumers.

In many cases, first parties and third parties must work together to provide consumers with appropriate notice, choice, control and to promote other responsible data practices. In the digital advertising space, a wide range of first and third parties cooperate to show consumers ads that are personalized to their interests. The NAI Code takes a FIPPs-based approach to ensure that these parties work together in the commitment to responsible data stewardship and privacy-protective practices. This is a model that a national privacy law should adopt.

2. Clarify individual control rights, which can create substantial challenges for authentication within the third-party advertising industry, and if not done effectively, could potentially lead to the collection of more personal information.

There is broad agreement that individuals should have the ability to exercise control over the use of their personal information, and that businesses should strive to provide reasonable consumer access to this data, depending on how the data is collected and used. In some cases, however, consumer access and deletion rights can be difficult to administer for third-party advertising companies. As discussed above, the NAI Code incentivizes member companies to avoid collecting personal information. This enhances privacy for consumers, but GDPR compliance efforts have shown that it also leads to challenges with respect to authenticating individuals for purposes of providing controls such as access, correction and deletion.

Companies that attempt to limit collection of information to non-personal information may need to obtain additional data—including personal information—in order to authenticate the identity of an online user seeking such access. Further, balancing the FIPPs with an outcomes-based approach, the

NAI believes it is practical to continue providing consumers with a choice to opt out of personalized advertising. However, GDPR-like rights for data deletion or correction for non-PI result in fewer benefits for consumers and should be weighed against the fact that these would likely lead to more collection of personal information, rather than less.

3. Allow publishers and service providers to charge a fee as an alternative to using a free, advertising supported model.

In addition to creating new rules for data privacy, both the GDPR and CCPA go one step further in seeking to establish new rights for consumers who make choices to limit their sharing of data. Both regimes support the idea that consumers who choose not to share their data with a service provider should not suffer a penalty for choosing not to share their data.

The CCPA's treatment of this issue is appropriate insofar as it recognizes that a company's provision of services to a consumer is not free of cost to the company, and that service providers have a right to require some form of compensation for their services if they cannot monetize through advertising. But by stating that the service provider can only charge a consumer for services in an amount equal in value to the data the consumer has withheld, the CCPA creates a form of rate regulation that will be tough to understand, and nearly impossible to coherently quantify or police. Further, unless the service is a necessary utility, a service provider should not be forced to provide services to anyone.

Given the central role of advertising-supported content on the Internet, and demonstrated consumer support for this model, it would be unfair and impractical to allow consumers to opt-out of an ad-supported funding model without allowing service provides to require the consumer to provide another form of compensation. Rather, companies should be free to offer whatever lawful services they choose over the internet, and to require whatever form of lawful compensation they choose in exchange for those services.

The CCPA approach to determining fair market value for the use of a consumers' data (e.g., for the purpose of providing personalized advertising) is not practical on a per-user basis, nor is it something that regulations are well suited to determine or require. In this case, the market is best suited to determining value through competing providers of Internet-based products and services using different revenue models.

IX. The FTC is well suited to remain the primary regulator of consumer privacy, but a federal privacy law should provide greater clarity around enforcement of unreasonable data practices and increased resources for FTC enforcement.

The FTC has been the chief federal agency for consumer privacy enforcement since the 1970s. Looking ahead, the FTC is well positioned to continue its data protection leadership in changing times through strong law enforcement, policy initiatives, and consumer and business education.[16]

As the Administration and Congress explore priorities for a federal data privacy law, the NAI believes that the FTC is well suited to leverage its longstanding experience and expertise to remain the primary administrator of consumer privacy and data protection laws. This should be done in a way that builds on the current risk-based approach, where FTC's jurisdiction over privacy matters complements, but it does not overlap or interfere with the jurisdiction of other federal regulators.

Additionally, a federal privacy law should provide for enforcement that is adaptable to changes in technology and consumer expectations, such as enabling the FTC to continue performing case-by-case assessments of information collection and use cases and assessing the potential for consumer injury in each case. In 2017, the FTC held a workshop and performed an assessment of these "informational injuries," but this effort warrants further consideration, as highlighted by the recent FTC staff report on this issue.[17] It could be beneficial for consumers and businesses to establish a reasonableness test that assess the uses of information, in conjunction with the type of information and the consumer harms and benefits, as well as the expectations of a reasonable consumer. This construct could be similar to—but more clearly defined—than the GDPR's establishment of "legitimate interest," providing for processing of personal data where consumers would expect, and that would not be deemed unreasonable.

The FTC, and consumers, would benefit from increased resources for enforcement. As one former Director of Consumer Protection has opined, "the Commission's ability to protect consumers in a time of rapid technological innovation depends on staying current with technological developments. The Commission cannot rest on its technological laurels but must continue to grow its technological resources."[18]

[16] See FTC overview of consumer privacy resources: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy, and catalogue of recent data privacy enforcement actions, guidance and educational resources for businesses and consumers: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises

[17] FTC Informational Injury Workshop: Bureau of Economics and Bureau of Consumer Protection Staff Perspective (October 2018). https://www.ftc.gov/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective

[18] David C. Vladeck, *Charting the Course: The Federal Trade Commission's Second Hundred Years,* 83 Geo. Wash. L. Rev. 2101-2129 (2015), available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/gwlr83&div=74&id=&page=

Conclusion

Again, thank you for the opportunity to provide comments on this important issue. The NAI supports the creation of a privacy law that enhances consumer privacy while balancing the need to promote robust innovation. We look forward to working with Congress and the Administration to advance this goal.