Hearings on Competition and Consumer Protection in 21st Century: Consumer Privacy, February 12-13, 2019

comments of the

Network Advertising Initiative (NAI)

filed with the

Federal Trade Commission

December 21, 2018

Thank you for to opportunity to submit comments in advance of the upcoming hearing on Consumer Privacy, scheduled for February 12-13. Please find below detailed responses to the questions for discussion at this hearing. In addition to these comments, the Network Advertising Initiative (NAI) would also welcome the opportunity to participate in the hearing. If you have any questions or would like to discuss these comments further, please contact David LeDuc, VP for Public Policy, at david@networkadvertising.org, or (703) 220-5943.

General Questions

Q: What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these benefits?

As the FTC staff recently noted in its comments to the NTIA, personalized advertising, which relies on collection of data from consumers, provides considerable value to consumers.[1] Today, a broad array of rich content is available on the Internet, including information and news content, video and music streaming services, and interactive 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 personalized advertising.

As the Internet-based media ecosystem has become richer and more diverse, one thing has remained constant: by far the most popular model among consumers is free or low-cost ad-supported content. While consumers do not necessarily recognize it, personalized advertising also provides for an improved user experience by increasing the relevance of advertising and decreasing the total number of ads displayed—essentially, it provides for replacing a large quantity of irrelevant advertising with a smaller quantity of advertising tailored to consumers interests.

The research below highlights the significant value consumers place on ad-supported content, and the value personalized advertising provides to consumers.

In late 2017, the NAI conducted an online consumer survey that obtained responses from 10,000 consumers from all demographics and geographic areas of the U.S. to assess their opinions on privacy, digital advertising, and the ad-supported Internet. The survey revealed that respondents overwhelmingly preferred their online content to be paid for by advertising, at a rate of 67%. This result was substantially consistent across all age groups.[2]

Additionally, 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.[3] 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 rate that has remained relatively flat over the past decade.[4] Nielsen's broad conclusion based on this research is as follows:

[1] FTC Staff Comment to the NTIA: Developing the Administration's Approach to Consumer Privacy (Nov. 2018).
[2] Digital advertising, online content, and privacy survey, Network Advertising Initiative (April 9, 2018).
[3] Nielsen Company, *As the Media Universe Grows, Ad-Supported Content Remains a Preferred Source* (March 14, 2018).
[4] Ibid.

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.[5]

While it is difficult to place a dollar value on the benefit that advertising-funded content provides to consumers, a survey commissioned by the Digital Advertising Alliance (DAA) revealed that consumers valued the cost of services like news, weather, video content, 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.

Q: The use of "big data" in automated decision-making has generated considerable discussion among privacy stakeholders. Do risks of information collection, sharing, aggregation, and use include risks related to potential biases in algorithms? Do they include risks related to use of information in risk scoring, differential pricing, and other individualized marketing practices? Should consideration of such risks depend on the accuracy of the underlying predictions? Do such risks differ when data is being collected and analyzed by a computer rather than a human?

The risk of bias cannot be completely eliminated whether data is being collected and analyzed by a human or using automated data analytics systems. However, protections under existing anti-discrimination and consumer protection laws already apply to the use of analytics in regulated eligibility contexts such as lending, insurance, housing, and employment, as covered by the Fair Credit Reporting Act (FCRA), Title VII of the Civil Rights Act, and the Equal Credit Opportunity Act (ECOA), among others. These protections also continue to apply to the use of data for personalizing advertising.

Interest-based advertising's utility is a function of its ability to differentiate between audiences with different interests. For example, a fashion brand seeking to reach an audience that would be interested in women's clothing benefits from being able to target its advertisements to a female, rather than a

[5] Ibid.
[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).

male audience. Or the same company might want to advertise retirement income products to older audiences. Distinctions like these are useful to both advertisers and consumers, and they do not present any discernible risk of consumer harm.

However, advertisements for some essential products or services should not be served in a way that results in discrimination affecting protected classes, and doing so is already illegal in the relevant contexts. For example, advertisements for housing that target audiences on the basis of race, religion, national origin, sex, disability, and familial status may be illegal under the Fair Housing Act. The Department of Housing and Urban Development (HUD) has fielded complaints involving the alleged use of online advertising to effect unlawful housing discrimination, which have resulted in increased compliance efforts.[8] Similarly, the EEOC administers a number of federal laws prohibiting discrimination in employment, and the has pursued allegations that employers have used online advertisements in a way that results in unlawful employment discrimination. In addition, the FTC already has the authority to pursue similar types of complaints with respect to advertisements for credit under the ECOA, as do state insurance regulators with respect to advertisements for insurance. Taken together, there is strong evidence that agencies such as HUD, the EEOC, the FTC, and others are well equipped to address complaints alleging unlawful discrimination from both traditional and algorithmic decision-making.

The NAI Code also works to prevent unlawful discrimination by prohibiting NAI members from using information gathered through personalized advertising to be used for determining employment, credit, health care, or insurance eligibility, areas where adverse outcomes could result. Given the combination of statutory and self-regulatory protections, the NAI does not see a present need for FTC or other policymakers to establish additional regulations pertaining to risks associated with algorithmic-based ad targeting.

Q: Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?

To be effective, privacy protections should be tailored to the sensitivity of data and the risk of consumer harm associated with the collection or use of those data. The NAI Code approaches this issue by distinguishing among several different types of data and assigning different levels of protection based on sensitivity. Under the Code, using certain categories of sensitive information for personalized advertising generally requires a user's Opt-In Consent. However, non-sensitive information associated only with a particular device (not a person) is less sensitive, and generally requires only opt-out consent under the Code.

The definition of "sensitive information" is therefore a critical element in promoting consumer privacy. The Commission has defined sensitive information to include financial information, health information, Social Security Numbers, and information about children.[9] In addition, responsible data stewardship is premised on responsiveness to reasonable expectations people have developed about the collection and use of information in different contexts.[10]

---

[8] Lane, Ben, *Facebook cuts thousands of ad targeting options after HUD's housing discrimination allegation*, HousingWire (August 22,2018).

[9] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 59 (March 2012).

[10] Mayer-Schönberger, Viktor; Cate, Fred; Cullen, Peter, *Reinventing Privacy Principles for the Big Data Age*. Oxford Internet Institute (December 6, 2013).

The NAI's definition of "Sensitive Data" goes further than the Commission's in several respects, and includes: Social Security Numbers or other government-issued identifiers; insurance plan numbers; financial account numbers; certain health-related information; and sexual orientation. Health-related information covered by the definition of "Sensitive Data" includes two categories of health-related data: (1) data about a health condition or treatment derived from a sensitive source; and (2) data about certain sensitive conditions regardless of the source of the data. Under the NAI Code, the collection and use of Sensitive Data for Personalized Advertising requires Opt-In Consent from individuals. The NAI Code also requires members to publicly disclose any standard interest segment they use for Personalized Advertising that are related to health conditions or treatments.

The Code also clarifies sexual orientation as "sensitive," prohibiting companies from collecting or storing information about an individual's status or perceived status as gay, lesbian, bisexual, or transgender for Personalized Advertising without obtaining that individual's Opt-In Consent.

While the Code does not explicitly classify information about children as "sensitive" as the Commission does, the Code does contain as separate requirement that any NAI member seeking to create an advertising segment specifically targeting children to obtain verifiable parental consent before doing so. The NAI Code also highlights the need for members to comply with the Children's Online Privacy Protection Act (COPPA) rules, which also undergo regular updates administered by the Commission.

In addition to distinguishing Sensitive Data from other kinds of information, the NAI Code distinguishes between Personally-Identifiable Information (PII), Precise-Location Data, Personal Directory Data, and Device-Identifiable Data (DII). The Code imposes appropriate notice and choice requirements for each category, providing a level of protection commensurate with the level of sensitivity of the data.

Adopting a poorly tailored approach to the treatment of sensitive information would be a disservice to consumers. For example, both the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have adopted an overly-broad definition of personal information that imposes undue burdens on business' legitimate processing of user data without providing any tangible corresponding benefit to consumers. In addition, a uniform level of protection for all categories of data provides no incentive for companies to use privacy-protective pseudonymous identifiers like IP addresses or device IDs instead of personal information like phone numbers or email addresses. 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.

The Commission should continue to examine practices involving sensitive information with special care. This and other critical definitions represent key areas where the FTC's enforcement experience and expertise can help to inform this discussion through policy papers that reflect the knowledge of leading experts and key stakeholders.

Q: Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?

Required privacy protections should allow for consumer variation in privacy preferences. For example, consumers who prefer free, ad-supported content that relies on the responsible use of data about them should not be prohibited from enjoying those services. Conversely, consumers who prefer subscription models should be able to choose those services and opt out of personalized advertising. Indeed, it is important to allow for competition among business models, which allows companies to provide free or low cost services for consumers that compete alongside subscription or license-based products, content, or software.

In 2016, FTC Consumer Protection Director Jessica Rich acknowledged that "consumers expect some level of data collection when they use their computer."[11] Still, consumers' values and expectations around data collection and use vary widely. Additionally, as technologies evolve to become more personalized and instrumental in all facets of our lives, consumer preferences and expectations of privacy are continuing to evolve over time, and consumers better understand data collection and use practices. Therefore, privacy protections should be sufficiently flexible to adapt to this environment.

The NAI Code of Conduct and associated guidance are premised on the principle that privacy protections should be flexible and capable of evolving over time to adapt to consumer preferences and expectations, while allowing innovative uses of data, including personalized advertising, which has been the lifeblood of the Internet ecosystem. For example, our opt-out requirement for Device Identifiable Information empowers consumers to choose whether data about them is used for Personalized Advertising.

In order to keep up with evolution in technology, the NAI produced new guidance this year to adapt the requirements of our Code of Conduct to smart TVs. This new guidance, in conjunction with our Code of Conduct, requires NAI members to provide transparency, notice and control for use of viewed content advertising.[12] Additionally, the NAI Code and related guidance have established a flexible approach for providing notice and consumer controls to protect consumers who use innovative mobile apps—this is a complex ecosystem requiring cooperation between app publishers, mobile operating system providers, and advertising companies. In addition to our robust set of privacy-protective requirements and detailed guidance for companies, the NAI is actively exploring opportunities, through additional guidance or changes to our Code, to ensure that users have better notice and more control regarding the sharing and use of their data, particularly their precise location data. For example, changes could include codification of some current NAI best practices, expanding NAI notice and choice requirements to also apply to real-time contextual use of location data, and expanding requirements to other sensors on mobile devices.[13]

The NAI Code and related guidance provide numerous examples of how industry self-regulation plays a critical role in helping consumers better understand new opportunities and uses of data, and to continue providing effective controls for the use of data about them. We believe this role will remain essential to guide the ad tech industry's compliance under a new federal privacy framework.

---

[11] Schiff, Allison, *The FTC Has Its Eye On What Smart TVs Mean For Consumer Privacy*, AdExchanger (December 8, 2016).
[12] NAI, Guidance for NAI Members: Viewed Content Advertising," (July 2018)
[13] NAI, How the NAI Helps Protect Consumer Location Data (Dec. 14, 2018)

Q: Market-based injuries can be objectively measured—for example, credit card fraud and medical identity theft often impact consumers' finances in a directly measurable way. Alternatively, a "non-market" injury, such as the embarrassment that comes from a breach of sensitive health information, cannot be objectively measured because there is no functioning market for it. Many significant privacy violations involve both market and non-market actors, sources, and harms. Should the Commission's privacy enforcement and policy work be limited to market-based harms? Why or why not?

In 2017, the Commission undertook a valuable exercise in assessing its deception and unfairness authority under Section 5, appropriately described in this context by then Acting Chairman Maureen Ohlhausen as an exploration of "informational injuries."[14] The Commission's authority in this area has proven to be quite broad, albeit challenging to apply in some cases where injuries are hard to identify. Based on a range of comments and discussion at the informational injury workshop, there appears to be broad agreement that privacy and data security incidents (involving various types of sensitive data) can and have caused injuries that do not involve solely financial loss. There was also substantial agreement that government intervention ought to be tied to injury, whatever the definition, and that countervailing benefits must be evaluated as well.

Given the various elements that contribute to the effort to measure injury, e.g. the type of injury, the sensitivity of the data, the magnitude, the frequency, and the causal link to a particular firm or practice, the NAI urges the Commission to continue assessing these on a case-by-case basis, with a thorough economic assessment of both risks and benefits to consumers and businesses. The NAI also supports the adoption of a framework to enhance accountability for the use of consumer data, such as new authority to assess data practices that are per se "reasonable" or "unreasonable." For example, such an approach could also address significant reputational injury.

Q: In general, privacy interventions could be implemented at many different points in the process of collecting, processing, and using data. For example, certain collections could be banned, certain uses could be opt-in only, or certain types of processing could trigger disclosure requirements. Where should interventions be focused? What interventions are appropriate?

As highlighted in our answers to various other questions, the NAI supports responsible data practices at multiple points in the process of collecting, processing, and using data. Three core functions that we provide are to (1) educate consumers, (2) provide consumers the ability to exercise choice, and (3) ensure member companies follow stricter requirements in circumstances that require additional privacy protection, including prohibitions on certain uses of data collected for personalized advertising. To educate consumers, we have an educational ad campaign that we run throughout the year, and we require member companies to provide clear and meaningful notice to consumers of their data collection and use practices. We offer an Opt-Out Mechanism for consumers to exercise their choice in receiving Interest Based Advertising from our member companies. In addition, the NAI Code, in certain circumstances, requires Opt-In Consent or additional disclosure requirements. For example, for sensitive categories (such as cancer, precise location, sexuality, etc.) we require Opt-In Consent, and we provide detailed guidance for use of robust notice if companies seek to collect this information. Finally, NAI

[14] Ohlhausen, Maureen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases* (September 19, 2017).

members are prohibited from using information collected for personalized advertising for determining employment, credit, health care, or insurance eligibility.

Q: Should policymakers and other stakeholders attempt to improve accountability for privacy issues within organizations? Why or why not? If so, how? Should privacy risk assessments be mandated for certain companies? Should minimum standards in privacy protections be required?

Accountability is a critical element of a risk-based privacy regime, and it is a key priority for the NAI and a requirement in the NAI Code. We require our members to take steps to bolster their privacy programs. Each NAI member company should designate at least one individual with responsibility for managing the member's compliance with the Code and providing training to relevant staff within the company. Members are also required to annually undergo reviews of their compliance with the Code by NAI compliance staff and other designees, as appropriate.

The NAI Code requires members to provide a mechanism by which users can submit questions or concerns about the company's collection and use of data for personalized advertising, and make reasonable efforts, in a timely manner, to respond to and resolve questions and concerns that involve the member company's compliance with the Code. We work with our members to ensure that they are complying with these accountability requirements in our Code and review their compliance during our annual compliance review process. Finally, our Code provides a process by which the NAI can refer members who violate the Code to the FTC for further enforcement procedures.

The NAI encourages the Commission and other policymakers to take efforts to improve accountability, including through support of the NAI code and similar self-regulatory approaches.

Q: How can firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data?

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. This is particularly true in the digital advertising space, where a wide range of first and third parties cooperate to show consumers ads that are personalized to their interests.

Although the NAI's membership is made up primarily of third-party advertising companies, our Code includes key elements that ensure trust and accountability for data transfers between first and third parties. For example, NAI members must contractually require any unaffiliated parties to which they provide PII for Personalized Advertising or Ad Delivery and Reporting purposes to adhere to the provisions of our Code concerning PII.

Additionally, our members must contractually require all parties to which they provide DII collected across web domains or applications owned or operated by different entities not to attempt to merge such DII with PII held by the receiving party or to otherwise re-identify the individual for Personalized Advertising purposes without obtaining the individual's Opt-In Consent.

While the Commission is wise to explore practices surrounding data transfers from first to third parties, it is critical to focus on what type of data each entity collects or processes, the purpose for which they were collected or transferred, the sensitivity of the data, and how the data are used and secured. The CCPA places an unnecessary and unhelpful emphasis on data transfers between first and third parties—

through an overly-broad definition of "sale"—rather than on collection and use, likely creating an unfounded fear around sharing with responsible third parties. This approach also runs the risk of creating 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.

The NAI encourages the Commission to promote responsible data sharing in order to enable robust growth and development of new technologies like artificial intelligence and machine learning, and making ad-supported content and services widely available to consumers.

What are the effects, if any, on competition and innovation from privacy interventions, including from policies such as data minimization, privacy by design, and other principles that the Commission has recommended?

Privacy by design and data minimization have become standard industry practices for companies that are committed to responsible data stewardship. However, these concepts require flexibility in their application to varying types of data and contexts, given that data innovation frequently arises from serendipitous use of data. Companies understand that it is in the interest of the consumer to retain data only for as long as it is reasonably necessary and to collect only the data that is relevant for a transaction. They also are disincentivized from collecting or retaining too much data because it poses a potential security risk.

The NAI Code divides data into three categories of "identifiability": Personally-Identifiable Information (PII), Device-Identifiable Information (DII), and De-Identified Data. This framework generally mirrors the "reasonable linkability" analysis set forth in the FTC Final Privacy Report.[15] This scaled approach recognizes that different categories of data present different levels of risk. The NAI believes that it is appropriate for the Code to continue to discourage members from linking the DII they collect with identified individuals for Personalized Advertising. To encourage these data minimization efforts, the Code continues to distinguish between PII and DII and to impose different notice and choice requirements for each, with the level of protection required increasing with the "identifiability" and sensitivity of the data.

Q: If businesses offer consumers choices with respect to privacy protections, can consumers be provided the right balance of information, i.e., enough to inform the choice, but not so much that it overwhelms the decisionmaker? What is the best way to strike that balance and assess its efficacy?

Transparency and control are fundamental pillars of the FIPPs, as well as the NAI Code. Of course, providing effective transparency and choice mechanisms can be difficult. The NAI spends considerable effort providing guidance to members about their notice mechanisms, and we provide a centralized portal offering information about Personalized Advertising, the requirements of the NAI Code, and information about and centralized access to user choice mechanisms. 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. The NAI continues to explore better ways to provide consumers with the right balance of

[15] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012).

information, including through robust, just-in-time notifications for the collection of more sensitive types of information such as personally identifiable information and precise geolocation information.

Q: To what extent do companies compete on privacy? How do they compete? To what extent are these competitive dynamics dictated or influenced by consumer preferences, regulatory requirements, or other factors?

Competition on privacy has increased along with consumer interest in the issue. Most companies recognize that the digital marketplace cannot be effective without consumer trust, and consumer trust cannot exist without adherence to privacy principles. The NAI is proud to be a driving force in market competition around privacy protections in third-party advertising. NAI members earn a more favorable position in the industry by adhering to stronger privacy protections, creating a growing incentive for other companies to participate in our self-regulatory program. In fact, membership in a self-regulatory program such as NAI's is a common contractual requirement among parties in the online advertising ecosystem. This framework encourages competition on privacy, while standardizing privacy practices, and we urge the FTC and other policymakers to promote industry self-regulation that furthers competition on privacy.

Q: Some academic studies have highlighted differences between consumers' stated preferences on privacy and their "revealed" preferences, as demonstrated by specific behaviors. What are the explanations for the differences?

As this question notes, there is often a gulf between consumers' stated privacy preferences and their "revealed" preferences demonstrated by their actions and behaviors. There are many possible reasons for this disparity, including survey questions that are not detailed enough to assess key aspects of consumers' privacy concerns. The online consumer survey conducted by NAI in 2017 revealed some interesting findings pertaining to consumer privacy concerns that could explain why consumers consistently express concerns about privacy when asked, but also continue to actively engage with websites, apps and internet services that collect data. When respondents were asked to share what they felt was the primary reason for their privacy concern on the Internet, 56% indicated that hackers were their top concern, while a combined 15% said that data collection by either the U.S. or a foreign government was their top concern. As a whole, concerns about data collection by hackers or government entities attribute to 72% of responses to this question. Only 8% of users were most concerned about website and application publishers collecting data, and 7% of users stated that data collection by advertising companies was their primary concern. Accordingly, it could be the case that consumers' concerns about data security and state-sponsored surveillance are the primary drivers behind their general privacy concerns.

Q: Given rapidly evolving technology and risks, can concrete, regulated technological requirements – such as data de-identification – help sustainably manage risks to consumers? When is data de-identified? Given the evolution of technology, is the definition of de-identified data from the FTC's 2012 Privacy Report workable? If not, are there alternatives?

Many consumer advocates, technologists, and regulators have adopted an overly strict view of de-identification, referring to any information that could possibly be linked to an identity as personal, essentially discrediting the term.[16] The NAI concurs with the conclusion reached by the Future of Privacy

[16] Narayanan, Arvind, Felten, Edward W., No silver bullet: De-identification still doesn't work (July 9, 2014).

Forum (FPF) in 2016 that while not foolproof, de-identification techniques unlock value by enabling important public and private research, allowing for the maintenance and use – and, in certain cases, sharing and publication – of valuable information, while mitigating privacy risk.[17] This conclusion is consistent with the FTC's 2012 Privacy Report and definition, which promoted de-identification.

The *Shades of Gray* paper proposes a sliding scale for calibrating legal rules to data depending on multiple gradations of identifiability, while also assessing other factors such as an organization's safeguards and controls, and it provides guidance on where to place important legal and technical boundaries between different categories of identifiability based on the presence of direct identifiers (*e.g.*, name, social security number) or indirect identifiers (*e.g.*, date of birth, gender) as well as technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals.[18]

Meaningful definitions for terms such as personal information," "sensitive information," and "pseudonymous data" are also critical 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. On the contrary, defining these terms to sweep in more data than necessary in an effort to protect consumers actually removes incentives for data de-identification, pseudonymization, and minimization. For example, any federal privacy law should encourage companies not to collect or use 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 PII given adequate time and resources. Our position is simply that those identifiers actually enhance privacy for consumers when companies do not link them to PII 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 PII. Combined with appropriate administrative controls that prevent inadvertent linking of such information to PII, this provides for a privacy protective environment.

The NAI urges the Commission to continue supporting policies that provide incentives for privacy protective practices, such as reliance on de-identified, pseudonymous and aggregate data.

[17] Polonetsky, Jules, Tene, Omer, Finch, Kelsey, Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification; Santa Clara Law Review (June 17, 2016).
[18] Ibid.

Questions About Legal Frameworks

Q: What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework? Does the need for federal privacy legislation depend on the efficacy of emerging legal frameworks at the state level? How much time is needed to assess their effect?

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 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 less than one year ago, 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.[19] Compliance costs were a major contributor to some U.S. sites going dark in Europe following implementation.[20] In many other cases, user experiences have been substantially degraded by redundant requests for consent. Additional research has recently found negative post-GDPR effects on EU ventures, relative to their US counterparts. [21] 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.[22]

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. Although it is hard to draw firm conclusions at this juncture, 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

[19] Smith, Oliver, Forbes, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown* (May 15, 2018).
[20] 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).
[21] 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
[22] Ibid.

new companies to enter the market, and for innovation to occur—and insist that competition be part of our conversation about privacy."[23]

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.

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.

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. Given the challenges that are apparent from the hastily-drafted CCPA, and the virtual certainty of additional conflicting state privacy statutes, there is little doubt that a patchwork of state privacy laws proliferating in the United States is an undesirable outcome for consumers, businesses, or regulators.

Q: If the U.S. were to enact federal privacy legislation, what should such legislation look like? Should it be based on Fair Information Practice Principles? How might a comprehensive law based on Fair Information Practice Principles account for differences in uses of data and sensitivity of data?

The NAI Code is rooted in the widely accepted FIPPs to govern the way that our members collect and use data for Personalized Advertising. The Code applies key 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. We believe that a FIPPs-based approach that focused on

[23] Phillips, Noah, *Keep It: Maintaining Competition in the Privacy Debate* (July 27, 2018).

preventing data harms would be effective for federal privacy legislation that protects privacy and encourages innovation. Such a FIPPs-based approach should be combined with industry self-regulation to best account for differences in the uses and sensitivity of data across large and diverse ecosystems for data collection and use.

To that end, the NAI urges 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 safe harbor program that exists under the Children's Online Privacy Protection Act (COPPA) provides one example of how this approach might work within a broad national privacy framework.

Adoption of safe harbors for robust privacy compliance programs could have several important benefits for Consumers and the Commission. 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 federal privacy laws. Second, safe harbors incentivize companies to invest time and resources into compliance. Third, they leverage the existing industry expertise and experience that is housed in long-standing self-regulatory organizations. 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 dozens of enforcement actions under COPPA, while safe harbor programs have worked continuously to promote and ensure compliance for hundreds of companies.

Q: Short of a comprehensive law, are there other more specific laws that should be enacted? Should the FTC have additional tools, such as the authority to seek civil penalties?

The NAI supports a national privacy framework, but we believe this should complement, rather than replace, the existing risk-based framework comprised of statutes such as HIPAA, GLBA, FCRA, COPPA, and other statutes enacted to address areas Congress has defined as sensitive. 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 consumer protection experience and technical expertise to remain the primary administrator and enforcement agency for consumer privacy and data protection. This should be done in a way that builds on the current risk-based approach, where FTC's jurisdiction over privacy matters complements, but does not overlap or interfere with, the jurisdiction of other federal regulators.

The NAI also supports the creation of a framework that enables the FTC to enforce a reasonableness standard that can establish a structured, public, and privacy-focused process for the Commission to follow in assessing data practices and protecting consumers.

The FTC, and consumers, would also benefit from increased resources for enforcement, as well as more resources for the FTC's international privacy staff that should increase efforts to harmonize privacy standards globally based on the US approach. 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."[24]

[24] David C. Vladeck, *Charting the Course: The Federal Trade Commission's Second Hundred Years*, 83 Geo. Wash. L. Rev. 2101-2129 (2015).