



February 18, 2011

Federal Trade Commission
Office of the Secretary, Room H-135 (Annex P)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Comments of the Network Advertising Initiative re Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

The Network Advertising Initiative ("NAI")¹ appreciates the opportunity to comment in response to the Preliminary FTC Staff Report.² The NAI commends the efforts of Staff to develop a cross-industry approach that promotes transparency and choice for consumers, while at the same time preserving online innovation and the benefits that flow to consumers from advertising-supported products and services.³

¹ The NAI is a coalition of 61 leading online advertising companies committed to developing actionable self-regulatory standards that establish and reward responsible business and data management practices and standards. The NAI maintains a centralized choice mechanism that allows consumers to opt out of online behavioral advertising by some or all of the NAI's member companies (at www.networkadvertising.org).

² Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010) (*hereinafter* "Preliminary Staff Report").

³ The NAI has previously commented on the importance of advertising revenue to sustaining the diversity of online services. *See* Comments of the NAI, Privacy Roundtables -- Comment Project No. P09541 (November 6, 2009), at 1-6, *available at* <http://www.ftc.gov/os/comments/privacyroundtable/544506-00019.pdf> (describing benefits of online behavioral advertising to consumers and publishers); Supplementary Comments of the NAI, Privacy Roundtables -- Comment Project No. P095416 (April 8, 2010), *available at* <http://www.ftc.gov/os/comments/privacyroundtable/544506-00117.pdf> (study data showing that behavioral-targeted ads sell for twice the price and offer twice the effectiveness of ordinary run-of-network advertising); *see also* Comments of the NAI, Privacy Roundtables -- Comment Project No. P095416 (Feb. 26, 2010), *available at* <http://www.ftc.gov/os/comments/privacyroundtable/544506-00099.pdf> (explaining self-regulation's role in protecting consumer privacy with respect to data collection and use for online behavioral advertising).

While recognizing that FTC Staff have already provided industry important guidance in its 2009 report,⁴ the NAI believes that its practical experience in implementing a voluntary code of conduct for online behavioral advertising (OBA) helps illustrate the importance of a flexible approach to applying any privacy framework. The NAI's comments address the proposed framework and Staff's questions from the general perspective of the online advertising marketplace. Additionally, the NAI's comments respond to Staff's questions relating to notice and choice mechanisms for online behavioral advertising.

1. Scope

As in its earlier report on online behavioral advertising, Staff's discussion of the proposed framework emphasizes the declining relevance of the distinction between personally-identifiable information ("PII") and non-personally identifiable information (non-PII). Since the establishment of its self-regulatory program in 2000, the NAI has long acknowledged that the collection and use of non-PII for purposes of interest-based advertising should be addressed from the perspective of consumers' privacy expectations. The provisions of the NAI Code applicable to uses of non-PII for online behavioral advertising adapt the Fair Information Practices Principles to the particular circumstances in which third parties collect and use interest-based data to serve advertising on first-party Websites.⁵

The scope of Staff's proposed consumer data privacy framework encompasses not just online advertising data, but all forms of commercial collection or use of data that "*can be reasonably linked to a specific consumer, computer or device.*" Data falling within the scope of the framework will require consumer notice and, if not a "commonly accepted practice," will also require consumer choice.⁶ As applied in an

⁴ See FTC Staff Report: *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), available at <http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf> (hereinafter "2009 OBA FTC Staff Report"). The Staff's OBA principles have helped establish the framework for the cross-industry program now being implemented, with the support of the NAI and its member companies. See *infra* at 10-11.

⁵ See NAI Code § III (imposing on member companies notice, choice, use limitation, access, reliability, and security requirements when collecting and using non-PII for purposes of marketing to users online). The NAI Code also emphasizes that relevant choices may vary depending on the type of data and its intended use in connection with online behavioral advertising (sensitive information, *e.g.*).

⁶ Under the proposed framework, notice for "commonly accepted practices" should occur in "*privacy policies in order to promote transparency and accountability,*" but should also be based on research to ensure that "*such privacy policies clearly and effectively communicate information to consumers that are not overly complex and likely to confuse.*" Preliminary Staff Report, *supra* note 2, at p. 54, n. 133 (emphasis added).

online context, such a framework creates a potentially strong presumption that all data collection of any type will require consumer notice: in order for the framework not to apply, the collecting entity would have to establish not only that the entity itself could not “reasonably” link the data to a specific consumer, computer or device, but also that any other person or entity subsequently having access to such data similarly could not “reasonably” link the data to the consumer, computer or device.

The “reasonably linked” approach in the framework does not expressly address other potentially relevant factors, including the intent of the collecting party (whether the collecting party intends to link the data to a specific consumer/device in the regular course of its business); the foreseeability that such linkage will occur (whether as a result of the acts of the collecting party, or the subsequent acts of any other potential user of the data, including users whose actions are unauthorized or exceed the scope of authorized use); the existence of contractual mechanisms that protect against linkage; and whether the potential privacy interest may vary depending on the nature of the consumer device to which the data is linked (for example, mobile phones vs. an Internet-enabled household device). Additionally, unlike the FTC’s existing approach to security-related issues, considerations of risk and potential harm resulting from “reasonable link[age]” are not expressly stated as relevant factors.⁷

Although the breadth of the scope of the proposed framework may be intended to promote privacy protection, as applied it could raise significant practical challenges for different industry sectors and companies seeking to provide consumer notice. Later in its discussion of simplified choice, the Preliminary Staff Report acknowledges that the intended uses of data may be material to the issue of appropriate consumer choice mechanisms. With respect to notice, however, the “reasonably linked” standard draws no similar distinction for data collection. This, combined with the absence of guidance on the other potentially relevant factors previously discussed, would create the possibility that far lengthier privacy disclosures would have to be provided by all data-collecting entities.

The potential for unnecessary disclosure that might result from general application of the proposed framework’s “reasonably linked” standard highlights the potential utility that self-regulatory mechanisms could play in fostering consumer awareness of data collection. Such mechanisms could more consistently identify and categorize for consumer notice the types of unique user data collected in connection with a particular business model; the technological standards applicable to determination of whether such data is or is not linked to specific consumers of such services or

⁷ The FTC’s flexible standard for consumer data security – reasonable safeguards dependent on the sensitivity of the data, size of the company’s operations, and the nature of risks faced by the company – has already proven its adaptability to a variety of industry sectors.

their devices (including future evolution of such technologies); other pertinent safeguards, such as contractual limitations on linkage; and additional relevant factors to determining the appropriateness of notice, including the potential materiality to consumers should linkage occur. Particularly where online data collection may involve multiple entities, self-regulatory frameworks can help more clearly allocate responsibility for providing appropriate notice. Companies adhering to a particular code of conduct would have the benefit of consistent guidance on how to provide consumer notice appropriate for that particular business model, rather than on an ad hoc basis. Additionally, the more detailed guidance that would result from a self-regulatory approach would help increase the likelihood that companies would reliably implement technologies designed to help maintain the anonymity of consumer data.

2. Privacy By Design: Organizational Adoption and Deployment

The Preliminary Staff Report identifies four substantive protections as a baseline for consumer data falling within the scope of the framework: companies should (a) provide reasonable security safeguards for their data; (b) collect information only to fulfill a specific legitimate need; (c) establish reasonable and appropriate data retention periods; and (d) take reasonable steps to ensure the accuracy of data.

As a general framework, these protections can constructively inform more detailed implementation through sector-specific standards developed through self-regulatory initiatives. Self-regulatory programs can not only evaluate how these general principles can be used to help establish specific codes of conduct for emerging services and technologies: such programs can also serve as an important vehicle for ensuring that participating companies share best practices about the actual means to implement “privacy by design.” In the NAI’s experience, the sharing of privacy-related practices fostered by self-regulatory initiatives is particularly useful to smaller companies. Smaller companies can leverage the expertise developed within a particular code of conduct in order to better instill privacy awareness among their employees throughout the lifecycle of data collection. Moreover, the commitment by companies in a particular industry sector to adhere to a privacy self-regulatory code can offer an efficient means of fostering the implementation of “Privacy by Design.” Having affirmatively promised to adhere to particular standards, companies must deploy internal resources necessary to address those commitments. Companies in self-regulatory programs face a variety of external accountability mechanisms. The combination of internal commitment and external verification helps ensure that companies consider privacy issues systematically as part of their everyday business.

The responses to some of Staff’s specific questions help illustrate how self-regulatory programs offer an effective path for implementing substantive privacy protections.

a. Incorporating Substantive Privacy Protections

The proposed framework's emphasis on the need to define a "*specific legitimate business need*" would be particularly relevant to online services in which the collecting entity seeks to notify consumers that there are multiple potential uses for the same data (*i.e.* where data collection occurs not only to provide and improve the product or service, but for operational purposes like fraud prevention and, potentially, for marketing purposes). However, in an interdependent online advertising ecosystem, it is less clear how this principle would provide guidance to multiple providers that already leverage consumer data for the business purpose of providing more relevant advertising to consumers.

Self-regulatory programs can address not only issues of legitimate business need, but other considerations that may potentially be material to consumers in the context of particular technological means of data collection and use. For data collected and used in online behavioral advertising, the NAI Code already requires that member companies must (a) provide reasonable security; (b) implement use limitations (including that members use such data only for marketing purposes); (c) establish a data retention period; and (d) take reasonable steps to ensure that such data comes from reliable sources.⁸ The Code requirement that data collected for online behavioral advertising purposes be used only for marketing purposes in particular shows how self-regulation can be adapted to provide substantive privacy protections across multiple entities' use of data.⁹ Moreover, the NAI program has also addressed the transparency of the technologies used for online behavioral advertising data collection. For example, when questions were raised as to the whether Local Shared Objects like Flash cookies were being used to undermine consumer preferences for online advertising, the NAI responded by adopting a policy broadly limiting the use of LSOs like Flash cookies until such time as Web browsers provide the same level of transparency and control currently available for standard HTTP cookies.¹⁰

The data retention principle in the proposed framework (that companies should define reasonable and appropriate retention periods) is another example of how

⁸ NAI Code § III(8) (reasonable security); § III(4)(use limitations); § III(7) (reliable sources requirement); and §§ III(9), 2(a)(vi) (retention standards).

⁹ NAI Code § III(4)(b). "Marketing Purposes" is defined as "any activity undertaken to collect, aggregate, analyze, maintain, update, or sell information in order to tailor content or services that allows or induces consumers to take action to purchase, rent, or exchange products, property or services, to solicit a charitable donation, to utilize market research or market surveys, or to provide verification services to marketers." *Id.* § II.9.

¹⁰ See NAI FAQ 19, available at http://www.networkadvertising.org/managing/faqs.asp#question_19.

self-regulatory approaches can further the goal of improved substantive privacy protections. For example, in the context of online advertising, there may be a variety of types of data that inform the selection of a particular ad to be shown to a particular user's browser, including demographic data (age or gender); short-term vs. long-term interest data (HDTV shopper vs. ski vacation package user); and other categories of inferred interest (technology products enthusiast, *e.g.*). Each of these data types may have different useful lifespans, but must also be stored in data systems that are subject to other business-related retention requirements. Variations in the type of advertising data relied upon by particular companies may lead to differing retention periods, with the result that there may be no single "reasonable" retention period. Nevertheless, on a sector-by-sector basis, self-regulatory frameworks can not only address how retention information can be made more transparent to consumers, but also establish best practices that normalize retention periods for particular classes of data.¹¹

b. Comprehensive Data Management Procedures

The Preliminary Staff Report points in an online context to the varying and potentially interdependent roles of browser vendors, website operators, and advertising companies. The NAI's experience in the context of online behavioral advertising corroborates the Staff's observations. The provision of enhanced notice and choice for online behavioral advertising (discussed in greater detail later in these comments) requires the cooperation of a full-cross section of the online industry: because of the interdependence of advertisers, Web publisher and advertising services providers must work collectively to provide consumers with transparency and control for the use of interest-based data.

The question of how best to implement management practices during the life cycle of data offers another example of how voluntary codes of conduct promote improved privacy practices. In the context of online behavioral advertising data usage, the NAI has recognized the potentially important role of contracts as an additional mechanism for data management. The NAI specifically imposes requirements that its members utilize contractual mechanisms in connection with their compliance efforts, including by imposing transfer and service restrictions. Self-regulatory programs thereby not only prescribe privacy requirements for their participating companies: they also broaden the scope of self-regulation by binding other companies to disclosure and data management requirements established under participating companies' standard form contracts. In this respect, a self-regulatory approach that supports such contract mechanisms can offer an important supplement to companies' unilateral efforts to establish comprehensive data management within their own data systems.

¹¹ The NAI Code specifically requires that member companies disclose the approximate length of time that they retain data collected for OBA and related purposes. Code § III(2)(a)(vi).

3. Simplified Choice

a. Commonly Accepted Practices

In proposing a framework to simplify choice for limited data practices, the Preliminary Staff Report identifies “commonly accepted practices” for which consumer consent will not be required: product and service fulfillment; internal operations; fraud prevention; legal compliance and public purpose; and first-party marketing. Many of these functions fall within the realm of what are also referred to as “operational purposes,” whether in an offline or online context. The framework also proposes that first-party marketing be considered a commonly accepted practice, but only if it based on consumers’ prior direct interactions with the company, or in online context, is solely contextual advertising. This proposed approach suggests that third-party data collection and use for advertising purposes should not be considered a “commonly accepted practice.”

Such a definition of “commonly accepted practices,” however, does not fully encompass the diversity of the online environment, where the provision of Web site content and advertisements will often involve entities that are not the same as the operator of the Web site through which content and advertisements are provided. Moreover, there are a variety of third-party advertising practices that do not rely on data previously collected concerning a specific consumer’s interests:

- General audience ads served by “third-party” advertising services providers in ad spaces that have not otherwise been sold by the Web site for brand awareness purposes (for example, movie ads preceding opening weekend);
- “Performance”-based ads for which the advertiser pays solely if the consumer responds to the ad by clicking or completing a purchase (for example, general interest ads for online education);
- Ads that are targeted solely on the basis of real-time information relating to the viewer of the advertisement, such as the time of day for that particular user (for example, breakfast specials at a fast food chain), or information inferred about the user’s general location from their browser’s IP address (for example, season tickets for the local hockey team);
- Ads served across pre-defined, “vertical” networks of Web sites where the general characteristics and subject matter of the participating sites – “fashion” or “auto interest” – signals the potential audience of their users in much the same way as special interest magazines attract subject matter-specific advertisers.¹²

These examples illustrate the potential limitations in an online context posed by a

¹² Staff’s contextual advertising definition speaks only to ads delivered “*where a consumer has direct interface with a particular company.*” Preliminary Staff Report, *supra* note 2, at p. 55, n. 134.

definition of “commonly accepted practices” that includes only “first-party” marketing.

Moreover, for these and other forms of online advertising carried out by third-party advertising services providers, there are a variety of operational purposes for data collection and use that are functionally the same as the first-party “commonly accepted” practices identified in the Preliminary Staff Report. For example:

- *Product service and fulfillment*: third-party advertising services providers must log data as a means of auditable proof to the advertisers that the impressions paid for have been delivered, or delivered to their intended audiences (including in particular “pay-for-click” ad campaigns);
- *Internal operations*: advertising providers deploy frequency capping to limiting the number of times a user sees the same ad, or serve a series of ads in a particular sequence (“storyboarding”); additionally, campaign performance data are gathered to measure the effectiveness of the creative;
- *Fraud prevention*: as is necessary for all forms of advertising, data must be logged to prevent click-fraud, or other forensic evidence of attempted abuse (attempts to distribute malware, *e.g.*);
- *Legal compliance and public purpose*: third-party advertising services providers may be obliged to maintain and or produce records relating to compliance with jurisdiction-specific requirements.

These examples help illustrate that the types of practices that Staff proposes be exempt from choice requirements (because it imposes more burden than benefit on both consumers and businesses) cannot necessarily be limited to bright-line distinctions between first-party and third-party data collection. Moreover, any proposed framework that seeks to define “commonly accepted practice” from a first vs. third-party perspective would also have to address other marketplace considerations, such as the comparative prevalence of usage of first-party vs. third-party advertising across the full spectrum of online products and services, including small and large-scale Web publishers.¹³ The “long tail” of the Web consists of millions of sites offering specialty content and niche services.¹⁴ Given the potential marketplace impacts that might result from uneven application of a “commonly accepted practice” standard across the long tail of online services, self-regulatory frameworks for particular business models of data collection and use may offer a more concrete approach to defining the appropriate circumstances in which

¹³ As discussed in the NAI’s prior comments, smaller Web sites may be more reliant on third party-mediated advertising services than larger scale publishers, due to their inability to rely on dedicated sales staffs to market their available inventory, or to achieve large-scale audiences that command advertising premiums.

¹⁴ See, *e.g.*, “What it takes to be a Top 100 Website,” available at <http://royal.pingdom.com/2010/07/05/what-it-takes-to-be-a-top-100-website-charts/> (data showing distribution of Web site usage along the “long tail”).

consumer choice should be provided.

b. Implementing Consumer Choice

The Preliminary Staff Report appropriately recognizes the challenges inherent in obtaining consumer consent in different contexts and on different platforms. The complexity of the online environment likely precludes any single format or approach to the technical mechanism for consumer consent across different business models. Distinctions will exist in the technological means by which companies collect and use data; where such data is stored (through local or host-based storage); the means for providing consumer notice through Web-based or locally-stored software mechanisms; and whether or not consumers interact with the product or service provider on an authenticated basis (*i.e.* whether the user registers and interacts with the product or service provider under expressly provided terms).

For online behavioral advertising, companies use the same technological mechanism – HTTP cookies – both as a means of delivering interest-based ads and of storing consumer preferences not to receive this type of advertising (“opt out cookies”).¹⁵ This has enabled self-regulatory programs (like the NAI and the Digital Advertising Alliance) to create integrated platforms that aggregate the choice mechanisms provided by multiple participants. Combined with a program of enhanced notice leveraging a common consumer icon to use these platforms, these self-regulatory programs offer a relatively standardized experience for users. Experience from the online behavioral advertising context shows how self-regulatory frameworks can craft integrated choice platforms that can be leveraged across multiple providers and platforms used for data collection and use. Such an integrated approach may be especially valuable for emerging challenges for consumer consent, such as choice options in a mobile environment that is characterized by a similarly diverse range of carrier, platform and services providers.

Self-regulation has also addressed the challenges of providing consent mechanisms that vary depending on the sensitivity and types of use of data. For uses of data for online behavioral advertising purposes, self-regulatory frameworks have taken a sliding scale approach to the appropriate consent mechanism: uses of data for

¹⁵ Industry has worked to develop easy-to-use tools to prevent users’ accidental deletion of opt out cookies, by providing browser add-ons that protect these cookies from removal. See, *e.g.* NAI Opt Out Protector for Firefox, http://www.networkadvertising.org/managing/protector_license.asp; Google’s “Keep My Opt Outs” plugin for Chrome, <https://chrome.google.com/webstore/detail/hhnjdpnhmckiecampfdgjlccfpfoe>. Furthermore, browser-related technologies already afford consumers independent mechanisms to exercise control over the storage of cookies.

online behavioral advertising purposes requires that consumers be provided with an opt-out choice mechanism, while uses of sensitive data require opt-in consent.¹⁶ The NAI Code details both the underlying definitions of the scope of online behavioral advertising as well as the differing types of sensitive information (financial, health, and precise location data, *e.g.*). Similarly, the NAI Code leverages other established consent mechanisms – such as COPPA’s verifiable parental consent requirement – in the context of use limitations on the creation of online behavioral advertising segments specifically targeting children under 13. While the particular approach to consumer consent mechanisms adopted in the context of one particular business model cannot be normalized across all forms of online data collection and use, the online behavioral advertising self-regulatory experience does demonstrate that self-regulation can appropriately provide differentiated consent mechanisms that recognize the potential sensitivity of certain classes of data.

c. “Do Not Track” as a Special Choice Mechanism for Online Behavioral Advertising

In its 2009 Report on Online Behavioral Advertising, FTC Staff established principles for consumer transparency and control: on all websites on which their data is collected for online behavioral advertising, consumers should be provided (1) a clear, concise, consumer-friendly and prominent statement that data is being collected for online behavioral advertising purposes, and (2) a clear, easy-to-use, and accessible method for choosing whether or not to have their information collected for such purposes.¹⁷ Noting the deficiency of lengthy privacy policies as a means for providing consumer transparency and control, the OBA Staff Report pointed to the potential promise of new forms of enhanced disclosure located in close proximity to online advertisements.

Since the issuance of that report, the NAI and its members have worked within the broader framework of cross-industry self-regulatory efforts to deploy such enhanced notice mechanisms for online behavioral advertising using a common, consumer-facing icon;¹⁸ to broaden the scope of participation in its existing self-regulatory framework for online advertising services companies engaged in online

¹⁶ See NAI Code § III(3); see also AAAA/ANA/BBB/DMA/IAB Principles, section III(A), VI(B) available at <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>.

¹⁷ 2009 OBA FTC Staff Report, *supra note 4*, at 46.

¹⁸ In October, the NAI joined other leading advertising and marketing associations in announcing the launch of a cross-industry program for self-regulation of online behavioral advertising, including a web site (www.aboutads.info) where companies can register to use an enhanced notice icon to be displayed within or near online ads or on Web pages where data is collected and used for interest-based ads. See <http://networkadvertising.org/pdfs/Associations104release.pdf>.

behavioral advertising; and to further expand comprehensive compliance and enforcement mechanisms.¹⁹

With respect to enhanced notice, NAI member companies have been leaders in initial deployments of enhanced notice mechanisms, having already served tens of billions of icon-based impressions that link consumers to specific disclosures describing their online behavioral advertising practices.²⁰ Additionally, other NAI member advertising services companies are now deploying on their ad delivery platforms the ability to enable the inclusion of the consumer notice icon within banner ads.²¹ Some NAI member companies have complemented these efforts to provide more ubiquitous notice with the introduction of ad “interest managers” that allow users to review the inferred interests associated with their browsers.²²

Moreover, the NAI has continued to expand the scope of its program and the reach of its consolidated opt out tool. Consumer usage of the NAI’s opt out tool saw rapid growth in 2010:

- Nearly three million unique visitors (2.84 million) viewed the NAI main Web page (an increase of nearly 150% over 2009);
- The number of unique visitors to the NAI’s opt out page rose to nearly 2.3 million unique visitors (an increase of 127% over 2009); and
- Approximately 472,000 unique users completed the NAI opt out process (an

¹⁹ The DMA has begun enforcing the Associations’ Principles for online behavioral advertising. See <http://www.the-dma.org/cgi/disppressrelease?article=1470>. Evidon, TRUSTe, and Double Verify have been approved as technology providers for compliance services.

²⁰ See, e.g., Google (<http://googlepublicpolicy.blogspot.com/2009/10/coming-to-online-ad-near-you-more-ads.html>); Yahoo (<http://www.ypolicyblog.com/policyblog/2010/10/05/nearing-one-trillion-impressions/>) (700 billion impressions); Microsoft (enhanced notice deployment on home pages of msn.com and bing.com).

²¹ See, e.g., AudienceScience (<http://www.audiencescience.com/adchoices>); Specific Media (<http://specificmedia.com/sites/privacy/>); MSN.com & bing.com (<http://choice.live.com/Default.aspx>); yahoo.com (<http://info.yahoo.com/privacy/us/yahoo/relevantads.html>).

²² See AOL AdVisibility Profile Viewer (<http://advertising.aol.com/advisibility>); BlueKai consumer preferences registry (<http://tags.bluekai.com/registry>); eXelate preference manager (<http://www.exelate.com/home/consumer-preference-manager-opt-out.html>); Google ad preference manager (www.google.com/ads/preferences); Lotame preferences manager (<http://www.lotame.com/preferences.html>); Microsoft Ad Preference Tool (<https://choice.live.com/UserPreferences>); Yahoo! ad interest manager (http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/).

increase of 58% over 2009).

Additionally, with more than 60 companies, the NAI's membership has more than doubled in the past 18 months, and now includes not just advertising networks, but also the leading data exchange and marketing analytics services providers.²³

Separately, NAI members have also participated in the launch of the Digital Advertising Alliance's cross-industry opt out platform (at www.aboutads.info). Like the NAI's opt out tool, the www.aboutads.info opt out mechanism allows consumers to opt out of online behavioral advertising by some or all participating companies. The www.aboutads.info platform is fully interactive with the NAI's opt out tool, allowing preferences set on either platform to be recognized and honored by a consumer's browser, and creating the opportunity for the consumer to set preferences for an even greater range of companies. Moreover, both platforms provide users with educational resources, access to company-specific privacy practices information, and explanations of the functioning and scope of these opt out choices.

With respect to the key indicia identified by FTC Staff – widespread adoption from both an industry and consumers – the combined self-regulatory efforts of industry have made very considerable progress towards the establishment of a uniform, comprehensive consumer choice mechanism for online behavioral advertising (sometimes referred to as “Do Not Track”). With respect to industry-wide participation, the accelerating scope of third-party advertising services providers' participation in either or both of the NAI and DAA programs illustrates that commitment to self-regulation of interest-based advertising is now becoming the industry “norm.” Furthermore, the available data show millions of users of existing opt out platforms like the NAI's, as well as significant additional usage of alternative mechanisms that leverage opt out mechanisms made available by industry participants in online behavioral advertising self-regulation.²⁴ Moreover, additional opt-out choices are becoming even more ubiquitously available through enhanced notice mechanisms and new, company-specific disclosure mechanisms. Collectively, these data demonstrate consumer knowledge and usage of the available choice mechanisms for interest-based advertising is already well established and rapidly expanding.

The deployment of enhanced notice mechanisms and the expansion of the footprint

²³ The NAI's membership includes the great majority of the marketplace for online behavioral advertising, including all 15 of the largest advertising networks. See http://www.comscore.com/Press_Events/Press_Releases/2010/1/comScore_Releases_December_2009_Ranking_of_Top_Ad_Networks.

²⁴ Preliminary Staff Report, *supra* note 2, at n. 70 (Citing 820,000 user downloads of TACO by Mozilla Firefox users and 250,000 users of the PrivacyChoice tool).

of the self-regulatory initiatives for interest-based advertising remains an ongoing process. Considerable challenges remain, such as determination of the applicability of principles of transparency and choice for behavioral advertising in the mobile context. Yet the enhanced notice initiative has already achieved extensive cross-industry coordination, including with respect to the exact format and placement of consumer-facing icon notices, and the technical means for conveying information relating to the companies responsible for a particular behaviorally targeted ad.²⁵ Moreover, existing self-regulatory initiatives have clearly and publicly defined the scope of their programs and of the relevant choices they provide to consumers with respect to online behavioral advertising.²⁶

As Staff reviews other potential approaches to the development of universal choice mechanisms, it should consider whether these alternatives would similarly secure cross-industry participation and implementation (recognizing the technical and consumer-messaging challenges involved); promote transparency as to the advertising services providers, Web sites, and advertising companies honoring the choice mechanism(s) and the relevant scope of the choices provided; the likelihood of broad participation and accountability within a corresponding self-regulatory enforcement scheme; and, of course, the marketplace impacts of any such mechanism(s), including any unintended impacts to the economic model for online advertising (not just online behavioral advertising).²⁷ Additionally, Staff will need to consider whether new choice mechanisms will complement the consumer's experience with established choice tools. And finally, Staff will also need to consider whether marketplace uncertainty as to the appropriate approach to choice mechanisms for online behavioral advertising would undermine the consensus necessary to achieve successful technical implementation of any one particular

²⁵ See, e.g., http://www.networkadvertising.org/pdfs/CLEAR_Ad_NoticeApril2010.pdf.

²⁶ As discussed previously, there remain a variety of advertising-related activities that do not involve the use of behaviorally-related data, as well as operational practices by third-party advertising companies that are closely analogous to first-party advertising.

²⁷ Because the average CPM paid for behaviorally-targeted advertising is twice as much as the average CPM for run of network advertising, a choice mechanism that severely limited the collection and use of data to provide relevant ads to users could limit the revenues that support online content and services. See Beales, "The Value of Behavioral Targeting" (March 2010), available at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. Another recent study demonstrated that important linkage between privacy regulation, the general effectiveness of ads served, and thus ultimately the price publishers can fetch for their inventory and use to pay for the content and services provided consumers. See generally Avi Goldfarb and Catherine E. Tucker, Privacy Regulation and Online Advertising (May 19, 2010), available at http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1611803_code512675.pdf?abstractid=1600259&mirid=1 (regulation in the EU marketplace that limits the use of ad targeting data estimated to reduce ad effectiveness by more than 60%).

mechanism.²⁸

4. Greater Transparency

a. Improved Notice and Access

As Staff notes, privacy policies have not fully met the challenge of communicating complex information about companies' data collection and use practices in a manner consumers can easily find and understand. Indeed, as noted above, it was FTC Staff's 2009 OBA Report's focus on the potential promise of new forms of enhanced disclosure²⁹ that provided impetus for the cross-industry effort by major advertising associations and the NAI to work to deploy such enhanced notice mechanisms for online behavioral advertising. In the context of online behavioral advertising, self-regulatory initiatives accordingly have begun standardizing the format through which consumers are provided access to information about online behavioral advertising practices and the choices available to them. As described above, industry is now deploying a common, consumer-facing icon that links consumers to short-form, consumer-friendly disclosures of material information relating to online behavioral advertising. In addition to the new short-form disclosures deployed by large portals like Yahoo and MSN, similar disclosures are now being deployed by major advertising networks.³⁰

These efforts demonstrate the potential for standardizing the format and terminology for conveying data practices for a particular business model or practice. For example, self-regulation has developed a standard icon for online behavioral advertising that may be extendable across industries as a means of *directing* consumers to privacy disclosures and choice mechanisms. Short-form disclosures such as those linked from the icon can then convey information about online behavioral advertising practices across websites and address similar questions using a common format. However, flexibility continues to be needed insofar as the companies making online behavioral advertising-related disclosures may also be attempting to convey additional information and choices about their general privacy

²⁸ A variety of new initiatives have emerged from browser providers that offer mechanisms for user control of third-party data collection and use. *See, e.g.,* <http://blogs.msdn.com/b/ie/archive/2011/02/10/acting-on-feedback-ie9-release-candidate-available-for-download.aspx> (official blog on IE9 beta release); <http://firstpersoncookie.wordpress.com/2011/01/23/more-choice-and-control-over-online-tracking/> (blog describing Mozilla header-based system for consumer choice). The details of these initiatives are still emerging and will require evaluation under the criteria outlined above.

²⁹ *See* 2009 FTC Staff Report, *supra* note 4, at 36-37.

³⁰ *See supra* note 21.

practices (for example, a publisher or service provider conveying other choices about the particular services and marketing it provides to its customers). There will be shared practices that are amenable to common terminology and disclosure, but there will also continue to be elements of disclosure that will be particular to the entity making disclosures. Nevertheless, for those industry practices for which common standards can be codified, self-regulatory programs can develop common terminologies for consumer notice and choice.

Another means of increasing transparency into data practices is through centralized choice mechanisms that present company-specific information for different organizations through a unified disclosure platform, as the NAI web site and www.aboutads.info do for online behavioral advertising. Such mechanisms provide “one-stop shopping” for online users to learn about the companies that collect data about their browsers, but with which they may not have direct relationships. Perhaps more importantly, at least in the case of such indirect third-party relationships, such centralized choice mechanisms also provide assurance to consumers that the participating companies follow a common set of rules governing choices relating to their collection and use of information.

With respect to access, some online technologies may be adaptable to providing consumers with improved transparency, but should be carefully calibrated so as to not inadvertently require increased data collection. With respect to online behavioral advertising, for example, HTTP cookies are used to collect and store predictive interest data to attempt to categorize and recognize similar groups of users, allowing online marketers to address “audiences” with advertisements for their products and services. Such cookies serve as the unique identifier used to gather and deliver interest-related advertisements. Several NAI member companies have leveraged this technology to provide users with the ability to view interest segments associated with their browsers.³¹ Significantly, it is the cookie identifier, not access to personally identifiable information, that facilitates such transparency. Accordingly, requirements of individual access are not necessarily practicable with respect to the underlying non-personally identifiable data used for online behavioral advertising purposes. A requirement to provide access to data associated with a particular online user (rather than browser) would necessitate data collection far exceeding the scope of data collection originally undertaken for advertising purposes.

b. Consumer Education

The Preliminary Staff Report emphasizes the desirability of education concerning specific business models, and the need to better explain to consumers the available

³¹ While this ability to provide access to non-PII associated with a browser has been implemented by some NAI member companies, the provision of such tools should be driven by self-regulation and market forces rather than regulation.

tools that they have to control the collection and use of data. Such consumer education is a necessary component of effective self-regulation. The NAI Code requires its members to make reasonable efforts to promote consumer education, and the NAI's companies have provided vigorous support in helping consumers discover and make use of the NAI's education resources for online behavioral advertising.³² In 2010, members contributed more than one billion online advertising impressions to the NAI's education efforts.³³ In 2010 alone, there were more than 500,000 unique visitors to the NAI's educational page, a several-fold increase from 2009. This number is greater than the number of unique visitors to the NAI page who completed opt-outs. Such data demonstrates the potential importance of education in helping consumers make informed choices, as well as the ability of self-regulatory programs to pool the resources of their members to achieve meaningful and consistent consumer communication.

* * *

The NAI appreciates the opportunity to respond to FTC Staff's questions, and looks forward to working with Staff as it evaluates the proposed framework and the appropriate role of self-regulatory approaches within that framework.

³² See http://www.networkadvertising.org/managing/learn_more.asp.

³³ The NAI's educational campaign complements the efforts of other industry associations, as well as of the company-specific efforts of participating members.