



January 28, 2011

Internet Policy Task Force
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, D.C. 20230

Submitted electronically to: privacynoi2010@ntia.doc.gov

Re: Commercial Data Privacy and Innovation in the Internet Economy: A
Dynamic Policy Framework (Docket No. 100402174-0175-01)

Introduction

The Network Advertising Initiative (“NAI”)¹ appreciates the opportunity to provide Comments to the Department of Commerce’s Internet Policy Task Force (“Task Force”) on its Green Paper, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.”² The NAI’s comments will address the Task Force’s questions relevant in the context of online behavioral advertising. Specifically, the NAI’s comments address (1) how the Fair Information Privacy Principles have helped inform sector-specific self-regulatory efforts like the NAI; and (2) how promotion by policy makers of such voluntary, enforceable codes of conduct can serve as the most effective means to enforce basic privacy principles and foster marketplace certainty, while at the same time securing deployment of

¹ The NAI is a coalition of more than 60 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 member companies (at www.networkadvertising.org). The NAI also filed comments in response to the Task Force’s NOI. See <http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Network%20Advertising%20Initiative%20Comments%2Epdf>.

² Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (December 2010) (*hereinafter* “Green Paper”).

innovative approaches to consumer transparency and choice in a dynamic technology marketplace.

I. Application of FIPPs for Sector-Specific Self-Regulation

The Fair Information Privacy Principles (FIPPs) serve as an important baseline that can instructively inform more detailed implementation of sector-specific standards developed through self-regulatory programs. The NAI's experience in applying the FIPPs' broad data protection principles also suggests that implementation of those principles still requires flexibility to adapt to varying types of data collection and use for particular business models and technologies.

The NAI's founding companies worked with the Federal Trade Commission (FTC) in 2000 to apply FIPPs to data collection and sharing by advertising networks serving online advertisements across Web sites. The NAI's 2000 Principles were the first online framework for self-regulation that explicitly addressed online uses of non-personally identifiable data ("non-PII data") for advertising. In December 2008, the NAI issued an updated Self-Regulatory Code of Conduct³ ("NAI Code") that more explicitly applied elements of the FIPPs to online behavioral advertising:

- Transparency and Purpose Specification⁴: the NAI Code requires members engaged in OBA to disclose their online advertising activities, the types of data collected, and how such data will be used, including any transfer. In addition to making such disclosures directly, member companies must require the websites where they collect data for online advertising purposes to make similar disclosures.⁵
- Individual Participation:
 - Consent: NAI members are required to provide Web users with access to a consumer opt-out mechanism for non-PII uses. Again, members must not only provide choice mechanisms directly on their own sites and the NAI's website, but also must require the websites where they

³ See the Network Advertising Initiative's 2008 Self-Regulatory Code of Conduct, available at http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf.

⁴ We refer to the DHS FIPPs used in the Green Paper, which are addressed to uses of personally identifiable information, and which the Task Force acknowledges may be subject to "some adjustment . . . or additional elaboration." See Green Paper at p. 26 & n. 73.

⁵ By obliging NAI members to require notice and choice provisions in their contracts with website partners, the NAI Code extends aspects of its self-regulatory regime beyond NAI membership to a larger footprint within the online advertising ecosystem.

contract to provide OBA services make available these choice mechanisms.

- Access: Members are required to provide reasonable access to any personally-identifiable information (“PII”) retained for OBA purposes (but not to non-PII retained for OBA purposes).
- Correction and redress: the NAI provides a means of accepting consumer complaints and requires members to respond to and make reasonable efforts to resolve consumer questions regarding compliance with the NAI Code.
- Data Minimization: The NAI Code provides incentives to collect only non-sensitive, non-PII. Members that use PII or sensitive consumer information for online behavioral advertising must obtain opt-in consent, whereas opt-out consent is required for the use of non-sensitive non-PII. The NAI Code also extends the Children’s Online Privacy Protection Act to the realm of non-PII, requiring verifiable parental consent for any use of non-PII to create an interest segment for behavioral advertising that is specifically targeted to children under 13. And the NAI Code requires members to retain data collected for online advertising purposes only for as long as necessary to fulfill a legitimate business need.
- Use Limitation: The NAI Code provides that members may only use, or allow the use of, consumer interest segments for marketing purposes.
- Data quality and integrity: The NAI Code requires members to make reasonable efforts to ensure that they obtain data for OBA uses from reliable sources.
- Security: Members are required to provide reasonable security for the data they collect, transfer, and store for online advertising purposes.
- Accountability and auditing: The NAI Code requires member companies to publically attest to compliance with the Code. These attestations are subject to enforcement by the Federal Trade Commission. Members are further required to undergo annual compliance reviews. Under the NAI Code, the results of the in-house compliance review and a summary of consumer complaints are required to be published annually.

The NAI Code accordingly sets minimum performance-based benchmarks that leverage the FIPPs principles, requiring participating members to weave these basic privacy protections into their business models.

The NAI Code helps demonstrate the appropriateness of flexibility in the implementation of FIPPs. The NAI Code was developed to address the particular issues related to browser-based collection of behavioral data for predictive advertising purposes. Inferred data relating to the likely interests of online users is used to attempt to categorize and recognize similar groups of users, allowing online marketers to address these “audiences” with advertisements for their products and services. The targeting of these audiences is not dependent on personally-identifiable information. Nor does the principal technology used for this type of advertising – HTTP cookies – require personally identifiable information in order to collect and store such predictive interest-related data. Such cookies, rather than the personal identity of the Web user, serve as the unique identifier used to gather and deliver interest-related advertisements.

Appropriate and tailored implementation of the FIPPs in an OBA context, accordingly, required their adaptation to “*correspond to the privacy risks provided by the[] service.*”⁶ Thus, to address marketplace concerns and promote consumer confidence, the NAI’s approach incorporates heightened consent requirements for potentially sensitive categories of data, as well as use limitations on non-marketing uses of interest-related data. Other aspects of the FIPPs, however, are less appropriate in the context of online behavioral advertising. For example, requirements of individual access are not practicable with respect to all data collected for OBA purposes, where such data is collected on a non-personally identifiable basis. To obtain data necessary to authenticate the identity of an online user seeking such access would necessitate data collection far exceeding the scope of data collection originally undertaken for advertising purposes.⁷ Moreover, the costs of implementing such a requirement would undermine the economic model through which OBA services enhance revenue to Web publishers.

Similarly, FIPPs-derived requirements of data correction predicated in users’ interest in the accuracy of their personal information would not be reasonably applied to predictive data inferred on a non-personally identifiable basis. Because better predictive data increases the likelihood of serving ads that will be relevant to consumers, NAI member companies have market-based incentives to ensure that the interest segment information is reliable. However, to the extent non-PII marketing data is “incorrect,” the potential harm that results to the user is the experience of receiving a less-relevant advertisement (similar to the experience for a user opted out of online behavioral advertising). Moreover, consumers have access to independent, browser-based mechanisms to remove their browser cookies correlated with any such data.

⁶ See Green Paper at p. 25 (“*Comprehensive baseline FIPPs would maintain the flexibility for each industry sector to develop tailored implementation plans that correspond to the privacy risks posed by their services.*”).

⁷ As is discussed later in these comments, what *is* feasible is the potential identification of the types of interest categories associated with a user’s browser.

A rigid framework involving equal application of all FIPPs to all types of data could also have the unintended effect of undermining other important individual data protection principles, such as data minimization. For example, as noted, the NAI Code implements FIPPs in the context of non-PII collected for online advertising purposes. One of the most important elements of the NAI Code is the incentive it creates for companies not to collect PII, and to ensure that any PII they collect for other purposes is not used for online advertising purposes. Companies that agree to abide by the NAI Code go to significant lengths to implement contractual and technical controls designed to ensure that they do not collect any PII, and to ensure that any PII they do inadvertently receive is not kept or used for online advertising. While it may be theoretically possible to link a given interest segment to an identifiable individual, member companies have significant incentives not to do so. Inflexible application of FIPPs that required identical protections for all types of data, whether personally identifiable or not, would provide no incentive to minimize data collection and use in this manner.

It is important to note, however, that flexibility need not come at the cost of meaningful data protection, oversight, and enforcement. Indeed, by tailoring FIPPs to the precise data, technology, and privacy risks at issue, self-regulatory codes of conduct like the NAI's impose meaningful commitments that alter marketplace behavior. And, as detailed below, the NAI couples self-regulatory oversight and enforcement with FTC deceptive practices authority, creating an effective accountability regime.

II. Transparency, Purpose Specification, Use Limitation, and Evaluation and Oversight

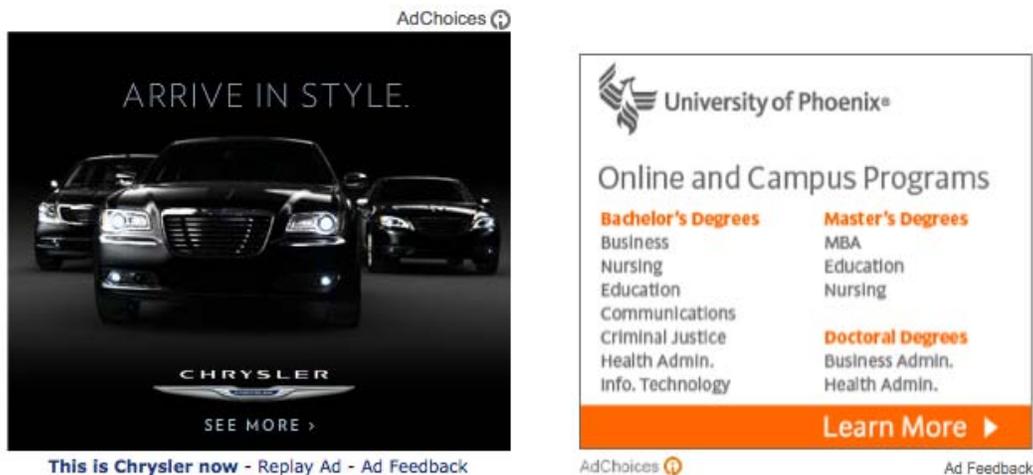
The Task Force rightly notes that that emphasizing certain data protection principles, including transparency, purpose specification and use limitation, and evaluation and oversight, can increase consumer understanding of data practices.⁸ Here too, the NAI's experience implementing these principles through a robust self-regulatory framework demonstrates the continued importance of flexibility.

A. Transparency

As the Task Force 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. In a 2009 report, FTC Staff noted the limitations of lengthy privacy policies as a means for providing consumer transparency and control over online behavioral advertising. The FTC report pointed to the potential promise of new forms of enhanced disclosure located

⁸ Green Paper at 30-31.

in close proximity to online advertisements.⁹ In response, the NAI and its members have worked within the broader framework of cross-industry self-regulatory efforts to deploy such enhanced notice mechanisms for OBA using a common, consumer-facing icon and messaging (“AdChoices”).¹⁰ NAI member companies have been leaders in initial deployments of enhanced notice mechanisms, having already served tens of billions of page and/or in-ad icon-based impressions that link consumers to specific disclosures describing their OBA practices.¹¹



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.

In addition to a consistent icon designed to promote consumer awareness, the enhanced notice program also leverages a short-form, consumer-friendly approach to disclosure of material information relating to online behavioral advertising. In addition to the new short-form disclosures deployed by large portals like Yahoo and

⁹ See FTC Staff Report: *Self-Regulatory Principles for Online Behavioral Advertising*, at pp. 36-37 (Feb. 2009), at <http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

¹⁰ See <http://networkadvertising.org/pdfs/Associations104release.pdf>. The NAI worked with other industry groups to launch www.aboutads.info, which allows consumers can learn about interest-based advertising and conveniently opt out of such advertising by some or all participating companies.

¹¹ 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/>) (tens of billions of user impressions delivered in 2010); Microsoft (enhanced notice deployment on home pages of MSN.com and bing.com).

MSN, similar disclosures are now being deployed by major advertising networks:¹²

The screenshot shows the AudienceScience website. At the top, there is a navigation bar with 'Contact Us', 'Careers', 'Client Support', and 'Client Login'. Below that, a secondary navigation bar includes 'ABOUT US', 'PRESS ROOM', and 'PARTNERS'. The main content area is titled 'Ad Choices: Learn More About Our Ads' and is divided into sections for consumers and advertisers. The 'For Consumers' section explains that advertising supports free content and services, and provides information on how ads are personalized based on online activity. It includes a 'Learn More!' box with links to 'www.AboutAds.info' and 'Network Advertising Initiative'. There is also a section for 'Where can I learn more about how AudienceScience selects ads?' with links to 'Privacy Policy Highlights' and 'Full Privacy Policy'. A 'To Opt-out of AudienceScience Network™' button is visible. The 'For Advertisers and Publishers' section mentions that AudienceScience provides audience targeting solutions.

The screenshot shows the Specific Media website's 'Privacy' page. The page title is 'Privacy' and the sub-header is 'Ad Choices Learn More About This Program'. The 'CONSUMERS' section explains that websites work with online advertising companies to provide relevant ads. It includes several questions and answers: 'How does online behavioral advertising work and what choices do I have?' with a link to 'www.aboutads.info'; 'Who placed this ad?' with a link to 'Specific Media'; 'Where can I learn more about what information Specific Media collects and how it is used?' with a link to 'Specific Media's privacy policies'; and 'What choices do I have about interest-based advertising from Specific Media?' with a link to 'Opt-out of receiving personalized advertising from Specific Media'. The page also states that Specific Media is the world's largest independent media platform and is committed to consumer privacy. At the bottom, it mentions that Specific Media is a member of industry organizations like NAI and IAB.

Other NAI member companies, together with a wide range of service providers affiliated with the cross-industry program, are now deploying such enhanced notice as an emerging marketplace “norm.”

¹² See Audience Science (<http://www.audiencescience.com/adchoices>); Specific Media (<http://specificmedia.com/sites/privacy/>).

Separately, as discussed in the NAI's prior comments, another transparency-related innovation developed by NAI member companies (and applauded by regulators) is the deployment of ad preference management tools that allow consumers to see and adjust the inferred interest segments associated with their browsers.¹³ The rapid adoption of preference managers illustrates how marketplace competition facilitates privacy-related innovation, and how self-regulatory frameworks like the NAI can facilitate adoption of such tools by smaller companies.

While short-form notices are potentially useful mechanisms for providing the most important information to consumers in an easy-to-understand manner, there remains an important role for full privacy notices. "Short form" notices, by necessity, simplify descriptions relating data sharing and use. Without full privacy policy disclosures, however, companies could be subject to claims of allegedly deceptive statements or omissions by virtue of attempting to communicate information to consumers in a user-friendly manner. And, as the FTC noted in its recent preliminary report, privacy notices continue to play a role in promoting companies' accountability and are useful for advocates, regulators, and consumers who want to learn more about a company's overall privacy practices.¹⁴

Recent innovations in delivering notice and choice to users in a consumer-friendly manner have been made possible by the flexibility and adaptability of self-regulation. Responding to concerns expressed by the FTC and privacy advocates, self-regulation has delivered both the means to provide notice in and around ads as well as consumer-facing platforms (the NAI's web site and www.aboutads.info) that offer easy-to-use solutions for managing online advertising preferences across a broad variety of companies. A key feature of the self-regulatory effort has been the integration between different market sectors: Web publishers, third party advertising services providers, and advertisers, are working collaboratively to deliver consumer transparency and choice.

The challenge in delivering consumer transparency across different market sector points to the potential limitations of an approach grounded in Privacy Impact Assessments (PIAs). Although potentially useful as a framework for helping a particular company review existing or potential uses of its own data, such a review would not necessarily provide similar transparency with respect to subsequent uses

¹³ For examples of preference management tools offered by NAI member companies, see 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/).

¹⁴ See Preliminary FTC Staff Report, *infra* note 10, at 70 (December, 2010).

of data shared with other companies. A self-regulatory approach focused on particular types of data that may be material to users – such as OBA – offers a greater potential of ensuring that all relevant marketplace participants involved in the particular practice will work to provide disclosures on a cross-industry basis. An emphasis on a cross-industry approach, rather than assessments by any one particular provider, is especially valuable when multiple providers may be involved in the delivery of the content and advertising for online products and services. Moreover, self-regulatory codes of conduct like the NAI’s require companies to build basic privacy protections into their business models. This forces participating members to “*identify and evaluate privacy risks arising from the use of*” information in adopting new technologies or information practices in the same manner as the PIAs contemplated in the Green Paper.¹⁵

B. Purpose Specification & Use Limitation

Self-regulation of online behavioral advertising demonstrates how companies can provide clear and understandable explanations of their data collection practices, and appropriately provide for choice mechanisms for data re-use. As noted above, the NAI Code requires member companies to describe their collection of data for online marketing purposes, and to require that the website publishers with which they work to also explain the data collection and use undertaken by third parties on their websites. The NAI provides sample language for websites to explain to visitors that their data will be collected for advertising purposes. And, as previously explained, such disclosures regarding the collection of data for online behavioral advertising purposes are increasingly available not only in privacy policies, but also through “short form” notices linked from icons placed in and around online ads. The NAI consumer website and aboutads.info similarly explain the purposes for which member companies collect OBA data from consumers, and how it is used for marketing purposes. Once collected for these explicitly-stated purposes, the NAI Code limits the use of that data other than for those purposes: member companies are prohibited from using, or allowing the use of, data collected for OBA other than for marketing purposes.

Self-regulatory programs also have the flexibility to implement limitation principles not just with respect to the particular kinds of data use, but also with respect to the technologies used to collect such data. In the OBA context, the means of data collection (browser-based) may be independently material to consumers, and as such can be addressed through codes of conduct. For example, as discussed in the NAI’s initial comments, when questions were raised as to whether Local Shared Objects (LSOs) like Flash cookies were being used to undermine consumer

¹⁵ See Green Paper at 34. The NAI supplements the work of its members in this regard, constantly engaging in dialogue with members about the application of the NAI Code to new technologies and services, and, when necessary, issuing formal policy guidelines addressing those issues.

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 browser tools provide the same level of transparency and control available today for standard HTML cookies.¹⁶ Broadly-based self-regulatory programs therefore offer the prospect of providing more timely application of use limitation principles.

C. Evaluation and Accountability

The Task Force rightly notes that a “*means of verifying – to people within an organization and to those outside—that an organization has observed its stated limits on data use is essential to building and maintaining consumer trust.*”¹⁷ Evaluation and accountability are crucial data protection principles. Self-regulatory groups can provide a flexible and yet meaningful means of verifying that a company’s data use is consistent with its self-regulatory obligations. The NAI, for example, employs a variety of means to verify that its members adhere to the privacy commitments embodied in the NAI Code, including: (1) public attestations of compliance with its Code of Conduct (enforceable by the FTC); (2) annual reviews of member companies; and (3) a mechanism for consumer questions and complaints relating to NAI compliance. In the event a compliance deficiency identified by any of these means remains unaddressed by a member, the NAI also retains the power to impose a range of sanctions, including referral to the FTC and suspension or revocation of NAI membership. Together, these tools create an effective accountability regime.

The primary means by which the NAI tests its members’ practices against their stated commitment to the principles contained in the NAI Code is through annual compliance reviews. In those reviews, the NAI engages in technical validation of members’ own descriptions of their business practices, such as by ensuring that opt out cookies are set properly and that their means for accepting and responding to consumer communications function appropriately. The compliance team questions technological representatives of member companies about relevant data flows, opt out functionality, data retention, and technical measures in place to prevent the use of any PII for OBA purposes. Separately, NAI compliance staff conducts independent tests of websites for the presence of appropriate notice and opt out mechanisms. In the event inconsistencies are found between the member company’s practices and the NAI Code, the NAI first asks the company to bring its practices into compliance with the Code. In the event the member company does not do so, NAI Staff may refer the company to the NAI Board for sanctions.¹⁸ The results of the

¹⁶ See http://networkadvertising.org/managing/faqs.asp-question_19.

¹⁷ Green Paper at 40.

¹⁸ The NAI believes that evaluation and accountability programs like the NAI’s annual reviews can be a more scalable and efficient means of ensuring compliance than formal audits requirements, which may not be economically feasible for smaller companies.

NAI's review are published annually, permitting public review of NAI Staff's findings.

Self-regulatory enforcement regimes like the NAI's complement governmental enforcement mechanisms, while at the same time alleviating the burden on limited government resources. The NAI receives thousands of consumer communications annually, providing consumers timely responses to these issues. Similarly, NAI Staff's annual compliance reviews allow for meaningful assessment of all participating companies' policies and practices – not only those who are subject to complaints or suspected of non-compliance – with respect to the handling of consumers' interest-related data. In these roles, the NAI provides meaningful oversight while freeing up FTC enforcement resources to address material threats to consumer privacy. At the same time, by requiring all members to publically attest to compliance, the NAI Code provides a basis for FTC enforcement in the event of non-compliance.

III. Voluntary, Enforceable Codes of Conduct: Promoting Industry Adoption and Marketplace Certainty

As previously discussed, the NAI's experience has been that self-regulation can best implement FIPPs in an efficient and meaningful manner. Moreover, as the Task Force notes, the NAI's "*voluntary, enforceable code of conduct*" is the result of a collaborative industry effort.¹⁹ Not only has the NAI continued to expand the scope of this code of conduct and the reach of its consolidated opt out tool: NAI members have also participated in the launch of the Digital Advertising Alliance's cross-industry principles program and its opt out platform (at www.aboutads.info). Like the NAI's opt out tool, the aboutads.info opt out mechanism allows consumers to opt out of online behavioral advertising by some or all participating companies. The 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.

The Digital Advertising Alliance program represents a further broadening of self-regulation for online behavioral advertising.²⁰ Industry groups representing all the components the online advertising ecosystem – publishers, advertisers, and the "third party" advertising services providers represented by the NAI (including ad networks, platforms, and exchanges) – have now signed on to voluntary, enforceable

¹⁹ Green Paper at 42.

²⁰ The "Associations Principles" were released in July 2009 by leading advertising industry associations to govern the collection, use, and transfer of information for OBA. See AAAA/ANA/BBB/DMA/IAB Principles, available at <http://www.thedma.org/government/ven-principles%2007-01-09%20FINAL.pdf>.

codes of conduct. The accelerating scope of third party advertising services providers' participation in either or both the NAI and DAA programs illustrates that commitment to self-regulation of interest-based advertising is now becoming the industry "norm." Consumer knowledge and usage of the available choice mechanisms for interest-based advertising are already well-established and rapidly expanding.²¹ Furthermore, because the Internet is by definition a global platform, development of a cross-industry approach to transparency and choice for OBA offers the prospect of a more harmonized international approach to self-regulation. Companies that implement enhanced notice mechanisms in the US market have strong incentives to leverage these mechanisms in other markets, thereby helping to promote global adoption of a self-regulatory framework grounded in the FIPPs.

The NAI's principles governing the collection and use of data for online behavioral advertising were developed, and continue to be developed, through consultation with non-industry stakeholders, including the FTC and privacy advocates, and thus can serve as a useful model for a multi-stakeholder process. The initial NAI Code of Conduct adopted in 2000 was developed in consultation with the FTC. In 2008, when revamping its Code of Conduct, the NAI put out a draft of its new code for public comment; the comments provided played a critical role in the ultimate Code of Conduct adopted. But this collaborative effort extends beyond the initial adoption of the NAI Code. The NAI continues engage in a dialogue with regulators and advocates concerning best practices for the protection of information collected and used for online advertising, and the NAI responds to and investigate as necessary complaints raised by consumers, the press, and privacy advocates. This input from consumers, policy makers, and industry is invaluable in identifying areas for the evolution of standards and best practices

A multi-stakeholder process, convened by the Department of Commerce through a new Privacy Policy Office, could usefully inform the existing cross-industry initiative for self regulation of online behavioral advertising. Such a process could factor in all relevant considerations, including consumer privacy concerns, economic costs and benefits, and impacts to innovation. However, any such multi-stakeholder process would also have to be calibrated carefully to preserve the existing accomplishments of self regulation. Very substantial industry investments have already been made to support the cross-industry programs, and continued deployment of a common architecture of enhanced notice will depend on marketplace certainty for its adoption. Any multi-stakeholder process should be designed to promote, rather than lessen, such certainty in the online marketplace (particularly given the

²¹ In 2009, there were more than one million visitors to the NAI's website. Nearly 300,000 unique visitors went through the NAI's opt-out process. *See* 2009 Annual Report, available at http://www.networkadvertising.org/pdfs/2009_NAI_Compliance_Report_12-30-09.pdf. Moreover, alternative mechanisms have emerged in the marketplace that further leverage opt out mechanisms made available by industry participants in OBA self regulation. *See* FTC Preliminary Staff Report at n. 70 (citing 820,000 user downloads of TACO by Mozilla Firefox users, and 250,000 users of the PrivacyChoice tool).

differing development cycles for evolving Web technologies). Similar weight for marketplace certainty should also be given to the relevant factors necessary to determine the success or failure of a multi-stakeholder process: given the complexity of the online ecosystem and the technological issues involved, such a process might produce consensus with respect to some issues, while continuing to require an iterative approach as to others.

Considerations of marketplace certainty for self-regulatory initiatives also should inform the Commerce Department's approach to the potential role of the states in the Dynamic Privacy Framework. Some of the same challenges that have arisen in the context of data security also apply in the privacy realm: in particular, how best to foster a consistent approach that successfully channels private-sector resources, while avoiding disparate standards that produce undue cost. Additionally, in contrast to data security, where the focus is on notice after the breach event, a data privacy framework places far more considerable emphasis on initial consumer disclosure and choice. In order to promote the goal of ease of consumer comprehension, privacy frameworks should as much as possible incorporate consistent approaches: in the OBA context, for example, industry is promoting a uniform consumer notice icon as a means of providing access to notice and choice. Given the already significant challenges to deploying such notice, the potential costs and benefits of a state-by-state approach should be weighed with respect to each of the material components of privacy frameworks.²²

* * *

The NAI appreciates the chance to comment on these questions, and looks forward to working with the Task Force as it continues to evaluate a Dynamic Privacy Framework.

²² Significantly, the states may exercise enforcement authority over deceptive practices. As with the FTC, self-regulatory codes of conduct that establish specific practice standards provide an important basis for continued oversight.