



March 2013 Draft Code of Conduct for Public Comment



1634 Eye St. NW, Suite 750, Washington,
DC 20006
www.networkadvertising.org

INTRODUCTION

The Network Advertising Initiative (“NAI”) is the leading self-regulatory body governing “third parties” in the online advertising ecosystem. The NAI is currently composed of more than 90 member companies and expanding. Since 2000, the NAI has imposed self-regulatory standards that establish and reward responsible business and data management practices with respect to the collection and use of data for online behavioral advertising (OBA) and related practices. The NAI Code, last updated in 2008, imposes notice, transparency, choice, and data security requirements on NAI member companies. Members are held to the promises they make to adhere to the NAI Code through a rigorous compliance and enforcement program that includes annual reviews, ongoing technical monitoring, mechanisms for accepting and investigating complaints of non-compliance, and sanction procedures.

The NAI believes that, like a successful privacy program, effective self-regulatory programs must constantly evolve to take into account changes in business models, technologies, and public policy. The NAI strives to stay abreast of all such changes and ensure that the substantive obligations imposed on member companies reflect the current landscape. To that end, in 2012, the NAI convened a working group composed of dozens of member companies. That group, NAI staff, and the NAI Board of Directors evaluated the current advertising ecosystem, convening numerous conference calls to discuss such topics as: (1) changes in the ecosystem that the Code should address; (2) notice requirements; (3) choice requirements; and (4) prohibited uses of data collected for OBA. This draft code is the result of that work. While much work has been done to develop the draft code, the work is not yet complete. The NAI welcomes the suggestions and feedback of others outside of the NAI on this draft code.

Purpose of this Revised Code

With this revision to its Code of Conduct, the NAI seeks to accomplish several goals. First, the NAI wants to ensure that NAI member companies continue to implement, honor, and maintain strong standards with respect to the collection and use of data for online advertising. The NAI recognizes the unique role that NAI members play in the Internet ecosystem. While our members are responsible for driving much of the revenue that allows web publishers and other “first parties” to provide the content and services that consumers enjoy for free, they also present unique concerns for some precisely because they lack a direct relationship with consumers. Even though NAI member companies primarily collect and use only non-personally identifiable information, we believe that the NAI must impose rigorous education, notice, and choice requirements. And, as noted above, we believe we must continue to adapt those requirements to ensure that our self-regulatory framework remains relevant and meaningful.

Second, the “third party” online advertising ecosystem has expanded and become more complex since the NAI last updated its Code of Conduct in 2008. At its inception in 2000 and into 2008, the NAI was composed primarily of “ad networks” that collected data across a network of websites for the purpose of serving ads based upon users’ presumed interests. Today, NAI membership is still composed entirely of “third parties” (or, in the case of some member companies, with the parts of the businesses that collect data as a “third party”), but the variety of business models is substantially more varied. NAI members today include not only ad networks, but also demand side platforms (DSPs), supply side platforms (SSPs), data management platforms (DMPs), data aggregators, ad exchanges, creative optimization firms, yield optimization firms, sharing utilities, and others. The NAI wants to ensure that it can welcome all third parties, and that its Code of Conduct is flexible enough to accommodate both existing and emerging third-party business models and practices.

Finally, since the NAI last updated its Code of Conduct in late 2008, there have been significant changes in the regulatory and self-regulatory landscape surrounding online advertising. Shortly after the NAI released its 2008 Code of Conduct, the FTC in February 2009 released a Staff Report setting forth a set of Self-Regulatory Principles for Online Behavioral Advertising. Those principles are substantially similar to the NAI Code, and the NAI has informally adopted those principles through its compliance program. Nevertheless, the FTC’s OBA Principles – and the “enhanced notice” requirement in particular – have not yet been formally codified by the NAI. In addition, also since the NAI last updated its Code of Conduct, the Digital Advertising Alliance (DAA) adopted, and has since begun enforcing, principles governing the collection and use of data for OBA. The DAA has also adopted a standard industry icon designed to inform users where ads are targeted to their interests. That icon, which is served trillions of times a month, is now an important component of self-regulation of online behavioral advertising practices.

Scope of the Draft Code

This draft code, like the current NAI Code, governs only NAI member companies. It does not govern all data collection by member companies, but is limited to their “Interest-Based Advertising” and “Ad Delivery and Reporting” activities as defined in this draft code. The draft code does *not* govern member companies’ activities insofar as they are acting as first parties or as “service providers” collecting and using data solely on behalf of a single first party. For example, a company collecting data on a single domain or set of affiliated domains for the purpose of conducting analytics would not be covered by the draft code so long as the data was not combined with data obtained on non-affiliated websites. To the extent a company collected data across non-affiliated websites, either for the purpose of engaging in Interest-Based Advertising or for Ad Delivery and Reporting across multiple websites, that activity *would* be governed by the NAI Code.

As of today, the NAI Code applies to members’ Interest-Based Advertising and Ad Delivery and Reporting Activities that: (1) occur in the United States or (2) apply to US consumers.

We encourage NAI members to apply the high standards of the NAI Code to these activities globally (and many member companies do so), but only U.S.-based online advertising activities are subject to the NAI compliance program today. Member companies are, of course, expected to abide by the laws applicable to their businesses. The NAI Code generally goes above the requirements of applicable laws. However, to the extent there is a conflict between the NAI Code and a member's obligations under applicable law, the member should abide by the applicable law.

While NAI members currently use cookies, javascript, and pixels for the activities governed by the NAI, the draft code is intended to be neutral with respect to the technologies used for Interest-Based Advertising. As behavioral advertising models expand beyond traditional desktop web browsing to mobile devices and tablets where cookies are often ineffective, companies may use other technologies to collect data and target ads. The NAI anticipates that such technologies, properly implemented, could also provide users an appropriate degree of transparency and control, and the principles contained herein are intended to apply regardless of the technology used.¹

Relationship to the DAA's OBA and Multi-Site Data Principles

As noted above, the Digital Advertising Alliance has developed and enforces, through the Better Business Bureau (BBB) and the Direct Marketing Association (DMA), a set of Principles governing the collection and use of data for OBA, as well as a set of Principles governing the collection of data across unaffiliated websites more generally.² The DAA is composed of six trade associations representing website publishers, advertisers, offline data providers, and the "third parties" represented by the NAI. As a result, its Principles for OBA and for Multi-Site Data collection govern the entire Internet ecosystem and impose obligations not only on third parties, but also on website publishers.

¹ This draft code of conduct is not intended to govern member companies' collection and use of data on mobile applications. It is, however, intended to establish baseline standards from which mobile application-specific guidelines can be developed. The NAI and other groups are in the process of developing guidelines that will specify the notice, choice, and other protections required of companies collecting and using data from mobile applications for Interest-Based Advertising and Ad Delivery and Reporting.

² See Digital Advertising Alliance, Self-Regulatory Principles for Online Behavioral Advertising (DAA OBA Principles), available at <http://www.aboutads.info/obaprinciples>; see also Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data (DAA Multi-Site Data Principles), available at <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

Because NAI member companies are bound both by the DAA's Principles and by the NAI Code, this draft code is intended largely to harmonize with the DAA's Principles as they apply to the OBA and Ad Delivery and Reporting by NAI member companies. Thus, for example, this draft code imposes an "enhanced" notice requirement for ads informed by Interest-Based Advertising and also makes explicit the "non-marketing purposes" for which member companies may not use, or allow the use of, data collected for advertising purposes (which also borrows from the DAA's Multi-Site Data Principles). As always, unlike the DAA's OBA Principles, the NAI Code applies only to NAI members,³ and only to the extent they are engaged in activities addressed by the NAI Code. As a result, obligations applicable to other companies in the advertising ecosystem contained in the DAA Principles are not included in this draft code. Similarly, obligations imposed on third-party advertising companies are in some cases phrased differently in this draft code than in the DAA Principles.

In some instances, this draft code (like the current NAI Code) imposes obligations on member companies beyond those required by the current DAA OBA and Multi-Site Data Principles. Those obligations include: (1) heightened notice and consent requirements for the merger of PII with Non-PII collected and used for "Interest-Based Advertising" (as defined in this draft code); (2) contractual notice requirements; (3) a requirement to provide transparency with respect to any health-related interest segments; (4) a requirement that the technologies used for Interest-Based Advertising and Ad Delivery and Reporting provide users an appropriate degree of transparency and control; (5) data retention limits and disclosure obligations; (6) reliable sources requirements; (7) limitations on the transfer of data collected for online advertising activities; and (8) access requirements for PII and associated Non-PII used for Interest-Based Advertising and Ad Delivery and Reporting. These additional obligations on NAI member companies ensure both consumers and companies that do business with third parties that NAI member companies implement, honor, and maintain the highest standards for data collection for online advertising – increasing trust across the entire ecosystem. Thus, the NAI Code complements and enhances the DAA Principles.

Framework of the Draft Code

The fundamental principle underpinning this draft code is that differing notice and choice obligations should apply depending on the sensitivity and the proposed use of the data. This basic principle, which has long been recognized by the NAI, is supported by the FTC

³ The current NAI Code and this draft code do promote some best practices for non-NAI member companies. For example, the NAI requires member companies to work with reliable sources and requires member companies to require their website partners to provide notice and choice on their sites. The NAI does not, however, impose any obligations on non-NAI member companies.

Final Privacy Report and the White House Privacy Report,⁴ both of which explicitly acknowledge that privacy protections should not be applied in a “one-size fits all” approach but should be flexible, scalable, and take into account the context in which the data is collected and used.

To that end, this draft code identifies three categories of data of varying levels of “identifiability” and imposes differing obligations on NAI members based on the sensitivity of the data and the proposed use. These three categories are: (1) Personally Identifiable Information (PII); (2) Non-PII; and (3) De-Identified Data. PII refers to data that is used or intended to be used to identify a particular *individual*; Non-PII refers to data that is not linked or reasonably linkable to an individual, but may be reasonably linkable to a particular *computer or device*; and De-Identified Data refers to data that is not linkable to either an individual or device. In addition, this draft code imposes obligations with respect to “Sensitive Data” and “Precise Geographic Location.” Sensitive Data is defined to include specific types of PII that are sensitive in nature, as well as health-related Non-PII. Precise Geolocation is a defined term under the draft code.

The current NAI Code of Conduct does not include commentary. We have added commentary to this draft code. The purpose of the commentary is not to add substantive obligations on member companies or to alter the principles set forth in the Code itself, but to explain the intent behind certain provisions of the Code. The commentary is also intended to provide examples of ways member companies can meet the substantive obligations of the Code.

⁴ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers* (March 2012) (FTC Final Privacy Report), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>; White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012) (White House Privacy Report), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

DRAFT 2013 NAI CODE OF CONDUCT

I. Definitions

A. Interest-Based Advertising

Interest-Based Advertising means the collection of data across web domains owned or operated by different entities for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected.

B. Ad Delivery and Reporting

Ad Delivery and Reporting is separate and distinct from Interest-Based Advertising and means the logging of page views or the collection of other information about a computer or device for the purpose of delivering ads or providing advertising-related services, including but not limited to: providing a specific advertisement based on a particular type of browser or time of day; statistical reporting in connection with the activity on a website; analytics and analysis; optimization of location of ad placement; ad performance; reach and frequency metrics (*e.g.*, frequency capping); security and fraud prevention; billing; and logging the number and type of ads served on a particular day to a particular website.

C. Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is any information used or intended to be used to identify a particular individual, including name, address, telephone number, email address, financial account number, and government-issued identifier.

D. Non-PII

Non-PII is data that is not PII as defined in the NAI Code, but that is linked or reasonably linkable to a particular computer or device. Non-PII includes, but is not limited to, unique identifiers associated with users' computer or devices and full IP addresses, where such identifiers or IP addresses are not linked to PII. Non-PII does not include De-Identified Data.

E. De-Identified Data

De-Identified Data is data that is not linked or reasonably linkable to an individual or to a particular computer or device.

F. Precise Geolocation Data

Precise Geolocation Data is information that describes the precise real-time geographic location of an individual derived through any technology that is capable of determining with reasonable specificity the actual physical location of a person or device at a specific moment in time, such as GPS level latitude-longitude coordinates or Wi-Fi triangulation.

G. Sensitive Data

Sensitive Data includes:

- Social Security Numbers or other Government-issued identifiers;
- Insurance plan numbers;
- Financial account numbers;
- Precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history; and
- Sexual orientation.

H. Opt-In Consent

Opt-In Consent means that a consumer takes some affirmative action that manifests the intent to opt in.

I. Opt-Out Mechanism

Opt-Out Mechanism is an easy-to-use mechanism by which consumers may exercise choice to disallow Interest-Based Advertising with respect to a particular browser or device.

II. Member Requirements

A. Education

1. Members shall collectively maintain an NAI website to serve as a centralized portal offering education about Interest-Based Advertising, the requirements of the NAI Code, and information about and centralized access to consumer choice mechanisms.

2. Members shall use reasonable efforts, both individually and collectively, to educate consumers about Interest-Based Advertising, and the choices available to consumers with respect to Interest-Based Advertising.

B. Transparency and Notice

1. Each member shall provide clear, meaningful, and prominent notice on its website that describes its data collection, transfer, and use practices for Interest-Based Advertising and/or Ad Delivery and Reporting. Such notice shall include descriptions of the following, as applicable:
 - a) The Interest-Based Advertising and/or Ad Delivery and Reporting activities undertaken by the member company;
 - b) The types of data collected, including any PII collected or used for Interest-Based Advertising or Ad Delivery and Reporting purposes;
 - c) How such data will be used, including transfer, if any, to a third party;
 - d) A general description of the technologies used by the company for Interest-Based Advertising and Ad Delivery and Reporting;
 - e) That the company is a member of the NAI and adheres to the NAI Code;
 - f) The approximate length of time that data used for Interest-Based Advertising or Ad Delivery and Reporting will be retained by the member company; and
 - g) An Opt-Out Mechanism.
2. Members that use standard interest segments for Interest-Based Advertising that are based on health-related information or interests shall disclose such segments on their websites.
3. Members shall require the websites where they collect data for Interest-Based Advertising to clearly and conspicuously post notice that contains:
 - a) A statement of the fact that data collection for Interest-Based Advertising is occurring;

- b) A description of types of data that are collected for Interest-Based Advertising purposes;
 - c) An explanation of how, and for what purpose, the data collected will be used or transferred to third parties; and
 - d) Where data will be collected for Interest-Based Advertising, a conspicuous link to the Interest-Based Advertising choice mechanism provided by the NAI member, and/or a conspicuous link to an industry opt-out page.
4. As part of members' overall efforts to promote transparency in the marketplace, members should make reasonable efforts to enforce contractual notice requirements and to otherwise ensure that all websites where they collect data for Interest-Based Advertising purposes furnish or require notices comparable to those described above.
5. Members shall provide, or support the provision of, notice of Interest-Based Advertising data collection and use practices and the choices available to users in or around advertisements that are informed by Interest-Based Advertising.

C. Consumer Control

1. The level of choice that members must provide is commensurate with the sensitivity and intended use of the data. Specifically:
- a) Use of Non-PII for Interest-Based Advertising shall require provision of an Opt-Out Mechanism, which shall be available both on the NAI website and on the member's website.
 - b) Use of PII to be merged with Non-PII on a going-forward basis for Interest-Based Advertising purposes (prospective merger) shall require provision of an Opt-Out Mechanism accompanied by robust notice of such choice.
 - c) Use of PII to be merged with previously collected Non-PII for Interest-Based Advertising purposes (retrospective merger) shall require a consumer's Opt-In Consent.
 - d) Use of Precise Geolocation Data for Interest-Based Advertising shall require a consumer's Opt-In Consent.

- e) Use of Sensitive Data for Interest-Based Advertising or Ad Delivery and Reporting shall require a consumer's Opt-In Consent.
2. When a user has opted out of Interest-Based Advertising, member companies must honor the user's choice as to the particular browser or device. Companies may continue to collect data for other purposes, including Ad Delivery and Reporting.
3. The technologies that members use for Interest-Based Advertising and Ad Delivery and Reporting purposes must provide users with an appropriate degree of transparency and control.

D. Use Limitations

1. Use of Non-PII or PII to create an Interest-Based Advertising segment specifically targeting children under 13 is prohibited without verifiable parental consent.
2. Members shall not use, or allow use of, data collected for Interest-Based Advertising or Ad Delivery and Reporting for any of the following purposes:
 - a) Employment Eligibility;
 - b) Credit Eligibility;
 - c) Health Care Eligibility; and
 - d) Insurance Eligibility and Underwriting and Pricing.
3. Members who make a material change to their Interest-Based Advertising data collection and use policies and practices shall obtain Opt-In Consent before applying such change to data collected prior to the change. In the absence of Opt-In Consent, data collected prior to the material change in policy shall continue to be governed by the policy in effect at the time the information was collected.

E. Transfer Restrictions

1. Members shall contractually require that any unaffiliated parties to which they provide PII for Interest-Based Advertising or Ad Delivery and Reporting services adhere to applicable provisions of this Code.

2. Members shall contractually require that all parties to whom they provide Non-PII collected across web domains owned or operated by different entities not attempt to merge such Non-PII with PII held by the receiving party or to re-identify the individual without obtaining the individual's Opt-In Consent. This requirement does not apply where the Non-PII is proprietary data of the receiving party.

F. Data Access, Quality, Security, and Retention

1. Members shall provide consumers with reasonable access to PII, and other information that is associated with PII, retained by the member for Interest-Based Advertising and/or Ad Delivery and Reporting purposes.
2. Members shall conduct appropriate due diligence to ensure that they obtain data used for Interest-Based Advertising from reliable sources that provide users with appropriate levels of notice and choice.
3. Members that collect, transfer, or store data for use in Interest-Based Advertising and/or Ad Delivery and Reporting shall provide reasonable security for that data.
4. Members engaged in Interest-Based Advertising and/or Ad Delivery and Reporting shall retain Non-PII and PII collected for these activities only as long as necessary to fulfill a legitimate business need, or as required by law.

III. Accountability

A. Member Obligations

1. This Code is self-regulatory in nature and is binding on all members of the NAI.
2. To help ensure compliance with the NAI Code of Conduct, each member company should designate at least one individual with responsibility for managing the company's compliance with the NAI Code and providing training to relevant staff within the company.

3. Membership in the NAI requires public representations that a member company's business practices are compliant with each aspect of this Code that applies to its business model, as supplemented by applicable implementation guidelines that shall be adopted by the NAI Board from time to time. Such representations involve explicit acknowledgement of NAI membership and compliance with the Code in each member's publicly available privacy policy, and inclusion in a group listing of participating companies on a designated page of the NAI website.

B. NAI Oversight

1. Members are required to annually undergo reviews of their compliance with the NAI Code by NAI compliance staff or other NAI designee. Members shall fully cooperate with NAI compliance staff, including in the course of annual compliance reviews and any investigation of a potential violation of the NAI Code.
2. The NAI's policies and procedures for annual compliance reviews and compliance investigations may be updated from time to time, and these policies and procedures shall be made available on the NAI website. These policies and procedures shall not only describe the process undertaken for a compliance review, but shall also articulate the penalties that could be imposed for a finding of non-compliance, including referral of the matter to the U.S. Federal Trade Commission.
3. The NAI shall annually post on its website a report summarizing the compliance of its members with the NAI Code and NAI policies, including any enforcement actions taken and a summary of complaints received.

C. Consumer Complaints

1. The NAI website shall include a centralized mechanism to receive consumer questions or complaints relating to members' compliance with this Code.
2. Each member shall provide a mechanism by which consumers can submit questions or concerns about the company's collection and use of data for Interest-Based Advertising, and shall make reasonable efforts to timely respond to and resolve questions and concerns that implicate the company's compliance with the NAI Code and NAI policies.

COMMENTARY ON DRAFT 2013 NAI CODE OF CONDUCT

I. DEFINITIONS

Interest-Based Advertising

This draft code replaces the term “Online Behavioral Advertising” (OBA) in the current NAI Code with “Interest-Based Advertising.” Interest-Based Advertising is defined as the collection of data across web domains owned or operated by different entities for the purpose of delivering advertising based on preferences or interests inferred from the data collected. Consistent with the NAI’s current Code of Conduct, the DAA’s OBA Principles, and the FTC’s definition of Online Behavioral Advertising, the draft definition of Interest-Based Advertising does *not* include “contextual advertising,” in which the ad selected depends upon the content of the page on which it is served, or “first party” marketing, in which first parties customize content or suggest products based upon the content of the website or users’ activity on their websites (including the content they view or the searches they perform).⁵ To the extent NAI member companies are engaged in such activities, those activities are outside of the scope of the NAI Code.

Online Behavioral Advertising and Interest-Based Advertising have always been understood to include the collection of data about a computer or device’s web viewing (or “click stream”) behavior over time to place browsers or devices into interest segments such as “car enthusiast” or “interested in travel.” With this new code, the NAI intends to make clear that Interest-Based Advertising also includes the practice known as “retargeting,” where the ad served on one website is selected based on a visit to a different website. For example, if a user visits SampleTravel.com, and then visits SampleNewspaper.com and is served an ad for SampleTravel based on the previous visit to SampleTravel.com, that activity falls within the definition of Interest-Based Advertising even though the ad was selected based on a single website visit and the user may not have been included in an interest segment such as “interested in travel.”⁶

PII, Non-PII, and De-Identified Data

This draft code divides data into three categories of “identifiability”: PII, Non-PII, and De-

⁵ See FTC Final Privacy Report, *supra* note 4, at 41; DAA OBA Principles, *supra* note 2, at 10-11 (defining OBA to exclude first party activity, ad delivery and ad reporting, and contextual advertising).

⁶ This approach is consistent with the FTC Final Privacy Report, where the Commission stated that it considers retargeting to fall within the scope of Interest-Based Advertising, not first-party marketing. See FTC Final Privacy Report, *supra* note 4, at 41.

Identified Data. Merger of PII with Non-PII for Interest-Based Advertising would require Opt-In Consent; use of Non-PII alone for Interest-Based Advertising would require notice and Opt-Out Consent; and use of De-Identified Data would not impose specific notice, consent, or data retention requirements. In addition, as discussed below, this draft code imposes obligations with respect to “Sensitive Data” and “Precise Geolocation,” both of which would require Opt-In Consent.

Under this framework, data would be considered PII if it is used or intended to be used to identify an *individual*, Non-PII if it is linked or reasonably linkable to a specific *computer or device*, and De-Identified Data if it is not linked or reasonably linkable to either an individual or to a specific computer or device. This framework mirrors the “reasonable linkability” analysis set forth in the FTC Final Privacy Report, which rejected a “bright line” test and instead adopted a scaled approach to evaluating risks and determining the obligations that attach to data.⁷ This scaled approach recognizes that different categories of data present different levels of risk.

The NAI Code has historically distinguished between PII and Non-PII and provided strong incentives for member companies to use only Non-PII for OBA and related purposes by imposing higher notice, choice, and access obligations for use of PII than for Non-PII. As a result of those incentives, the vast majority of NAI member companies collect only Non-PII for OBA purposes. Those companies that do collect PII for non-Interest-Based Advertising purposes remove any PII before using Non-PII associated with that PII for OBA purposes, and no member companies currently merge PII with Non-PII data collected for OBA purposes.

Recently, regulators have raised questions about the utility of maintaining the traditional distinctions between PII and Non-PII.⁸ Despite the increasing difficulty in drawing bright lines between PII and Non-PII, however, we believe it is appropriate for the NAI Code to continue to encourage the efforts of member companies to take express steps to prevent the Non-PII they collect for Interest-Based Advertising and Ad Delivery and Reporting purposes from being linked to particular individuals. To encourage these data minimization efforts, this draft code continues to distinguish between PII and Non-PII 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. At the same time, this code provides additional guidance with respect to the meanings of each term, to help ensure that data is treated appropriately.

⁷ See *id.* at 19-20 (acknowledging commenters’ concerns that requiring the same level of protection for all data might undermine companies’ incentives to avoid collecting data that is easily identified).

⁸ See *id.* at 18-19.

PII

The draft definition of PII - any information used or intended to be used to identify a particular individual, including name, address, telephone number, email address, financial account number, and government-issued identifier – is similar to the current definition of PII in the NAI Code, except that it eliminates data used or intended to be used to “precisely locate” an individual. The NAI believes that this language was needlessly confusing and irrelevant, because the definition of “Sensitive Data” requiring Opt-In Consent includes data used to determine the precise location of an individual or device. In addition to the examples of PII enumerated in the draft definition, PII could include new technologies not currently in use for Interest-Based Advertising. For example, “faceprints” would be considered PII to the extent a company employed facial recognition technology for the purpose of identifying individuals, even if such faceprints were not linked to name, address, telephone number, email address, or other traditional identifiers.

Non-PII

Non-PII is defined in the draft code as follows: “data that is not PII as defined in the NAI Code, but that is linked or reasonably linkable to a particular computer or device. Non-PII includes, but is not limited to, unique identifiers associated with users’ computer or devices and full IP addresses, where such identifiers or IP addresses are not linked to PII. Non-PII does not include De-Identified Data.” In order for data to be treated as Non-PII under this draft code, the company would need to (1) take measures to ensure that the data cannot reasonably be linked to a particular individual, (2) publically commit to maintain the data as Non-PII, and (3) contractually prohibit any companies with whom it shares the Non-PII from attempting to merge the data with PII or otherwise using the data to identify a particular individual (unless the Non-PII is proprietary to the receiving party). We elaborate on each of these measures below.

Measures to ensure that Non-PII cannot reasonably be linked to a particular individual: Measures a company could take to ensure that Non-PII cannot reasonably be linked to a particular individual include using only randomly generated numeric identifiers rather than names or other personal information.

Public Commitment to Maintain Data as Non-PII: The company must publicly commit to maintain and use Non-PII and not attempt to link the Non-PII to PII or to a particular individual. For NAI members, consistent with section II(B)(1)(b), this will require a statement in the member’s privacy policy that the company collects only Non-PII, describes the types of Non-PII it collects and uses for Interest-Based Advertising and related purposes, and commits to maintaining the data’s Non-PII state (and not to merge the Non-PII with PII). Consistent with section II(C)(1)(c), NAI members would be required to provide notice and obtain Opt-In Consent if they later wished to merge the Non-PII with PII

or to identify the individual from the “Non-PII” data set.

Contractual Prohibitions on Merging Non-PII with PII or Attempting to Identify Individuals: If the company shares Non-PII data that the receiving party could reasonably link to an individual, it must contractually prohibit the receiving entities from attempting to link the Non-PII to PII or to a particular individual without obtaining a user’s Opt-In Consent as required for retrospective merger of PII and Non-PII under section II(C)(1)(c). Companies should also avoid providing such recipients with the means to identify an individual from the data set. For example, with respect to encrypted data/identifiers, companies should not disclose the algorithm or other mechanism used to render the data Non-PII. These requirements would not apply when the Non-PII transferred is proprietary to the receiving party. Thus, for example, where an NAI member company collects Non-PII on behalf of a single client, it would not be required to forbid that client from merging the Non-PII with any PII it may hold.

De-Identified Data

This draft code imposes notice and choice obligations with respect to the collection of “Non-PII,” but also contemplates that member companies may collect and use De-Identified Data for which notice and choice is not required under this draft code. For example, once member companies no longer need Non-PII for Interest-Based Advertising or Ad Delivery and Reporting purposes, they may de-identify that data and use it for aggregate reporting. Similarly, member companies may collect or receive data that was never associated with a particular computer or device.

This draft code defines De-Identified Data as data that is not linked, and cannot reasonably be linked with, an individual or with a particular computer or device. In order to be considered “De-Identified Data” under the NAI Code, the company must take steps similar to those enumerated above with respect to Non-PII: (1) take reasonable steps to ensure that the data cannot reasonably be re-associated or connected or associated with an individual or with a particular computer or device, such as by removing or hashing the cookie identifier or IP address, or truncating the IP address; (2) publicly commit to maintain and use the data in a de-identified fashion and not attempt to re-associate the data with an individual or with a particular computer or device; (3) obtain satisfactory written assurance that any non-affiliate that receives the De-Identified Data will not attempt to reconstruct the data in a way such that an individual or computer or device may be re-identified and will use or disclose the De-Identified Data only for uses specified by the NAI member company. This process mirrors the definition of “De-Identification Process” in the DAA’s Multi-Site Principles.⁹

⁹ See DAA Multi-Site Data Principles, *supra* note 2, at 8.

Sensitive Data

There is general consensus that information about children under the age of 13, financial and health information, Social Security numbers, and precise geolocation is “sensitive” and accordingly entitled to greater protections.¹⁰ The 2008 NAI Code and this draft code accord each of these categories of data heightened protection, and require companies to obtain Opt-In Consent to use each type of data for Interest-Based Advertising (which, in the case of children’s data, must be obtained from the parent in accordance with COPPA standards as set forth in section II(D)(1) of this draft code).

The draft definition of “Sensitive Data” is similar to the definition of “Sensitive Consumer Information” in the current NAI Code, but makes precise geolocation a separate category of data (that also requires Opt-In Consent) and adds sexual orientation as a new category of sensitive data.

Health

It is difficult to draw bright lines between “sensitive” and “non-sensitive” data in the health space. Whether a particular piece of data is sensitive may lie in the eye of the beholder and depend upon a number of subjective considerations.¹¹ In recognition of that subjectivity, and following commentary provided in response to our draft 2008 Code, the NAI has not developed an exhaustive list of conditions or treatments that it considers to be “precise.”¹² Rather, the NAI requires companies to consider a number of factors in determining whether a particular condition or treatment is “precise” and therefore requires a company to obtain Opt-In Consent if it wishes to serve ads based on presumed interest in the topic,¹³

¹⁰ See FTC Final Privacy Report, *supra* note 4, at 59.

¹¹ See, e.g., *id.* at 60.

¹² The 2008 NAI Code was always intended to require Opt-In Consent to target users on the basis of any presumed interest in, as well as actual knowledge of, “precise” health conditions or treatments, not merely actual knowledge that the user suffers from such condition. Nevertheless, there has been considerable confusion among member companies and others on this point. See, e.g. <http://blog.privacychoice.org/2011/12/14/yet-another-better-definition-of-sensitive-boundaries-for-ad-targeting/> (stating that the NAI’s standard applies only to the actual health status of the user). With this commentary, the NAI intends to make clear that targeting users on the basis of any presumed interest in, not merely actual knowledge of, precise or sensitive health-related topics requires Opt-In Consent.

¹³ These requirements apply only to the extent member companies are collecting data to associate users with presumed interests. They do *not* apply to members’ services that do not require tagging users’ browsers or devices, such as categorizing websites associated

including: the seriousness of the condition, its prevalence, whether it is something that an average person would consider to be embarrassing, whether it is treated by over-the-counter or prescription medications, and whether it can be treated by modifications in lifestyle as opposed to medical intervention. Under this analysis, all types of cancer, mental health-related conditions, and sexually transmitted diseases are “precise” and would require Opt-In Consent. Other conditions, such as acne, high blood pressure, heartburn, cold and flu, and cholesterol management, the NAI considers to be generic and not topics that require Opt-In Consent.

The NAI has also adopted a policy requiring member companies to publicly disclose any standard interest segments they use for OBA that are related to health conditions or treatments. Section II(B)(2) of this draft code would codify that requirement. Together, the two sections require members to obtain Opt-In Consent to serve ads on non-affiliate websites that are based on presumed interest in precise or sensitive health conditions or treatments (whether through “standard” interest segments, custom segments, or retargeting), and to disclose (and provide an Opt-Out Mechanism for) any “standard” interest segments that are based on non-precise, non-sensitive, health-related interests.

Sexual Orientation

This draft code adds sexual orientation as a category of sensitive data that requires Opt-In Consent. Though sexual orientation was not included in the categories of data requiring Opt-In Consent under the 2008 Code, the NAI believes there is now greater consensus around treating sexual orientation as sensitive data. Indeed, in the FTC’s 2009 OBA Report, FTC staff noted that commenters had listed “sexual orientation information” as a category of information around which there “appears to be consensus that such data merits some form of heightened protection.”¹⁴ Under this revision, companies would be prohibited from collecting or storing information about a user’s sexual behavior or orientation for Interest-Based Advertising or Ad Delivery and Reporting without obtaining Opt-In Consent.¹⁵

with particular conditions or treatments so that advertisers can serve contextual advertising on those sites.

¹⁴ Federal Trade Commission, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, at 42 (February 2009) (“FTC 2009 OBA Report”), *available at* <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

¹⁵ Similarly, tagging visitors to websites designed for GLBT users, such as same-sex dating or travel sites, for purposes of later retargeting those users or placing them into an interest segment that identifies the sexual orientation of the user would not be permitted without Opt-In Consent.

Precise Geolocation

Since 2008, the NAI has accorded precise geolocation data special treatment by including such data in the definition of “Sensitive Consumer Data” for which Opt-In Consent is required. This draft revision removes “precise geolocation” from the definition of sensitive data, but continues to require Opt-In Consent for use of that data. This heightened level of consent recognizes that such data can, for example, be used to build detailed profiles of consumer movements over time and to identify individuals using disparate pieces of data. The definition of “Precise Geolocation” in this draft code is intended to provide clarity with respect to the type of location data that requires Opt-In Consent and to recognize that a range of technologies now and in the future may be able to provide “with reasonable specificity” the actual physical location of a device at a specific moment. At the same time, the definition is intended to *exclude* more general geographic location data, such as IP address-derived location, postal code, zip code, city, and neighborhood.

II. MEMBER REQUIREMENTS

Education (§ II(A))

Consumer education is a crucial component of the NAI Code. Although no new substantive requirements have been added in this draft code, the section has been labeled as “Education” rather than “Transparency” and the language has been modified to focus on educating consumers to be consistent with the DAA’s OBA Principles.

Member-Provided Notice (§ II(B)(1))

This draft code, like the current NAI Code, would require companies to provide clear, meaningful, and prominent notice concerning their data collection practices. To meet the “prominent” requirement, companies should provide conspicuous links to their consumer-facing disclosures, such as obvious links to privacy policies, “consumer information” links, and independent links to Opt-Out Mechanisms. Links to privacy policies and other consumer-facing materials (such as an opt-out page) should be in a location that is easy for users to locate, in an appropriate size font, and in a color that does not blend in with the background of the page.

To meet the “clear and meaningful” requirement, the notice should describe the company’s data collection and use practices in an understandable manner and accurately reflect the company’s data collection and use practices. In describing the types of data they collect, members that obtain data from third parties for purposes of supplementing user profiles should disclose the data they collect and how they use it for Interest-Based Advertising.

Finally, members should describe their data collection and use practices in as clear and concise a manner as possible. The NAI has long encouraged as a best practice short, clear,

and concise privacy notices that communicate to users in plain English how the company collects and uses data for OBA purposes. Throughout the compliance review process, NAI staff regularly encourages members to streamline their privacy policies consistent with this best practice recommendation.

This draft code adds a requirement that members disclose the technologies used by the company for Interest-Based Advertising and Ad Delivery and Reporting. This provision is intended to bring an additional level of transparency to all technologies members use for those purposes (e.g., cookies, pixels). The provision is *not* intended to require member companies to disclose the technologies they use with a level of specificity that would reveal their proprietary business models.

Health Transparency (§ II(B)(2))

In 2011, the NAI adopted a policy requiring members to publicly disclose all standard interest segments used for online behavioral advertising purposes that are based on health-related interests. The NAI adopted this policy because we believe that an additional layer of transparency for health-related segments helps to promote compliance with Code requirements, normalize best practices by all participants in the online advertising ecosystem, and enhance users' confidence that sensitive health-related information is not collected and used without their knowledge and consent. Such transparency also allows users to make more educated decisions about whether to opt out of the collection of data for Interest-Based Advertising purposes by some or all NAI member companies. This policy, which has already been implemented by many NAI member companies, would be codified in section II(B)(2) of the revised Code.

Under the current NAI Code and section II(C)(1)(e) of this draft code, member companies continue to be required to obtain Opt-In Consent for the collection and use of "Sensitive Data" for Interest-Based Advertising or Ad Delivery and Reporting, which is defined to include "precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history." As a result, if an NAI member company were to seek to serve ads to users on the basis of knowledge of a user's health condition or treatments or presumed interest in sensitive health conditions such as cancer, mental health-related conditions, or sexually transmitted diseases, the company would need to clearly explain that intent and obtain Opt-In Consent for such use. The transparency requirement, by contrast, is intended to capture those interest segments for which Opt-In Consent is not required under the Code, but nevertheless may factor into an individual's decision about whether to opt out of Interest-Based Advertising by a particular member company. Thus, for example, member companies may seek to target users on the basis of such general health categories as headaches, allergies, or diet and fitness that would not require Opt-In Consent under the NAI Code, but would require disclosure under the transparency policy. The disclosure may be in, or linked from, the member's privacy policy, in other consumer-facing materials, such

as a preference manager, or in another location on the member’s website that is reasonably easy for users to find.

In addition to disclosing their standard interest segments that are related to health conditions or treatments, members are expected to have internal policies governing any use of health-related targeting. Many NAI members do not have “standard” interest segments, but rather engage solely in retargeting, keyword retargeting, or the creation of “custom” segments. Other members do have standard interest segments, but also allow their clients to create custom or retargeted segments. In all such cases, members must ensure, consistent with Section II(C)(1)(e), that they obtain Opt-In Consent for any targeting (including retargeting or custom segments) that is based on “precise” health conditions or treatments. In addition, they should publicly disclose their policies for targeting based on any health-related interests.

Website Notice (§ II(B)(3)-(5))

Contractual Notice Requirements (§ II(B)(3)-(4))

Under the 2008 Code and this draft code, NAI members must contractually require their website partners to provide notice concerning data collection for Interest-Based Advertising. Those requirements are intended to ensure that consumers are provided notice of data collection by NAI member companies on the websites they view, which NAI members generally do not control and where they lack the ability to provide notice directly to consumers.

Since the NAI last updated its Code in 2008, the DAA developed and now enforces its own set of Principles governing the collection and use of data for OBA purposes. Those principles require website publishers to provide notice of OBA data collection occurring on their sites independent of any contractual requirements imposed by NAI members.¹⁶ Despite the fact that website publishers now have an obligation to post notice of OBA data collection under the DAA Principles (where the third party does not provide such notice) independent of contractual requirements imposed by NAI member companies, the NAI continues to believe that, where an NAI member company has a direct contractual

¹⁶ Section II.B of the DAA’s OBA Principles, which governs website publishers as well as the third-party entities represented by NAI membership, requires that when data is collected from or used on a website for OBA purposes, the operator of the website include a clear, meaningful, and prominent link on the webpage where data is collected or used for such purposes that links to a disclosure that describes the OBA taking place, states the adherence to the Principles, and contains an opt-out mechanism. This disclosure is not necessary when enhanced notice may be provided either in or around the ad, or on the web page where data is collected. *See* DAA OBA Principles, *supra* note 2.

relationship with a website where it collects data for Interest-Based Advertising, it must contractually require the website to post notice of Interest-Based Advertising data collection and link to an Opt-Out Mechanism.¹⁷ The draft code also states that members should use reasonable efforts to enforce those contractual notice provisions, as well as to ensure that notice is provided even in the absence of a contractual requirement to provide such notice. Members can meet this requirement by, for example, regularly checking a reasonably sized sample of the websites where they collect data for Interest-Based Advertising to ensure that they provide appropriate notice and following up with those that do not.¹⁸

Enhanced Notice Requirement (§ II(B)(5))

This draft code would require members to provide, or support the provision of, notice of Interest-Based Advertising data collection and use practices and the choices available to users in or around advertisements that are informed by Interest-Based Advertising. This provision is intended to add an “enhanced notice” requirement to the NAI Code for the first time. NAI members largely already provide, or support the provision of, notice in or around ads. Indeed, NAI member companies, together with the DAA, were instrumental in the deployment of in-ad notice. By requiring notice both in privacy policies and other footer links as well as in and around ads, member companies can help to ensure that consumers are provided notice both at the time of data collection (through privacy policies) and at the point of data use (when ads that informed by Interest-Based Advertising are served).¹⁹

¹⁷ The requirement to contractually require a website publisher to post notice applies only where the NAI member itself is collecting data. Some member companies do not themselves collect data, but facilitate others’ collection of data for Interest-Based Advertising purposes, such as by providing software or other technology that allows others to collect such data. In such cases, the NAI encourages, but does not require, members to ensure that proper notice is provided where their technology is used to collect data for Interest-Based Advertising purposes.

¹⁸ The contractual notice provisions are intended to ensure that users are provided notice at the point of data collection, even where there is no ad served. Some member companies may collect data for Interest-Based Advertising purposes only where they serve ads. Member companies who provide in-ad notice pursuant to section II.B(5) and only collect data for Interest-Based Advertising where they serve ads will ensure that notice is provided wherever they collect data for Interest-Based Advertising, and need not contractually require their website partners to provide notice or enforce contractual notice requirements.

¹⁹ The FTC has remarked upon the need for flexibility in the timing and format of notice provided to consumers, noting that in some contexts, it may be more practical to communicate choices after data collection has occurred. The Commission noted in

The draft enhanced notice language states that members “shall provide, or support the provision of” notice in or around the ads they serve. This language is intended to make clear that all NAI members must participate in in-ad notice programs, but also to recognize that some companies will not be able to provide such enhanced notice because of where they sit in the ecosystem. The NAI expects that companies who lack the ability to include the standard industry icon or other form of enhanced notice on ads will nevertheless support the provision of such notice by configuring their systems to support that capability. In addition, if a publisher or advertiser asks an NAI member to conduct a campaign informed by Interest-Based Advertising without enhanced notice, the NAI member should decline to conduct the campaign and should report such advertisers and publishers to the BBB or DMA compliance program.²⁰ The NAI will work with DAA and DAA member organizations to educate advertisers and publishers on the requirements of the DAA program, including the requirement that all Interest-Based ads include enhanced notice.

Choice (§ II(C))

Provision of Choice Mechanisms (§ II(C)(1))

Since 2000, the NAI has required its members to provide a means for consumers to exercise control with respect to the collection and use of data for online behavioral advertising purposes. Members are currently required to provide such mechanisms on their own websites and on the NAI website, and also now provide those mechanisms on the DAA’s opt-out page, aboutads.info. As explained in the previous section of this commentary, the current NAI Code and this draft code put obligations on member companies to ensure that their website publisher partners provide links to these choice mechanisms on the websites where member companies collect data for Interest-Based Advertising purposes, and this draft code also requires notice of data collection and choice options through in-ad notice.

The NAI believes that member companies should continue to be required to provide Opt-Out Mechanisms for the collection and use of data for Interest-Based Advertising purposes. At the same time, this draft code, like the current NAI Code, requires Opt-In Consent for the use of Sensitive Data and Precise Geolocation. Similarly, this draft code requires Opt-In

particular OBA, where in-ad notice provides a “teachable moment” for consumers to make decisions about their data, even though a cookie often has already been placed. *See* FTC Final Privacy Report, *supra* note 4, at 50.

²⁰ Similarly, because enhanced notice will now be a requirement of the NAI Code, the NAI will have authority to enforce the enhanced notice requirements against NAI member companies under its compliance and enforcement program.

Consent for the retrospective merger of PII and Non-PII for Interest-Based Advertising purposes. For the prospective merger of PII and Non-PII for Interest-Based Advertising purposes, this draft code requires the provision of an Opt-Out Mechanism coupled with “robust” notice. To be considered “robust” under this provision, such notice must be provided immediately above or below the mechanism used to authorize the submission of any PII. The notice should also clearly and conspicuously describe the scope of any Non-PII to be merged with PII and how the merged data would be used for Interest-Based Advertising purposes.

Honoring Opt-Out Choices (§ II(C)(2))

The current NAI Code requires member companies to “provide and honor” users’ opt-out choices. This draft code continues to require members both to “provide” and to “honor” choice, but breaks the “honor” requirement into a stand-alone provision. This change is intended to accomplish two goals: (1) to emphasize the importance of honoring users’ opt-out choices; and (2) to make clear that members may in the future be required to honor users’ choices even when those choices are expressed through mechanisms that member companies do not themselves “provide.”

Section II(C)(2) is also intended to provide further clarity and certainty with respect to what it means to “honor” users’ opt-out choices. Following an opt out, companies must cease collecting and using data for Interest-Based Advertising purposes, but may continue to collect data for other purposes. It is widely acknowledged that certain commonly accepted “internal operations” practices should not require consumer choice and thus that collection of data for such purposes following an opt out is permissible. Such purposes include frequency capping and similar advertising inventory metrics.²¹ They also include calculating usage statistics and verifying ad delivery.²² This draft code accordingly would allow member companies to continue to collect data for such purposes following a user’s choice to opt out.

While companies may continue to collect and use data for purposes other than Interest-Based Advertising following an opt out, their opt out mechanisms must be consistent with the representations they make to consumers and to NAI staff. The NAI works with each member company during the pre-certification and annual review processes to ensure that its opt out, at minimum, stops the collection of data across unaffiliated domains for purposes of delivering advertising based on inferred or known preferences or interests. Some companies’ opt-out tools cover activity that does not squarely fall within the

²¹ See FTC Final Privacy Report, *supra* note 4, at 39.

²² See *id.* at 12 (stating that data collection for such purposes may not require companies to provide “extensive options for control”).

definition of “Interest-Based Advertising” as defined in this Code. The NAI expects that companies’ opt outs will be consistent with the representations made to NAI staff and in their privacy policies and will hold companies accountable for their representations through the NAI’s sanctions procedures.

Technologies Used for Interest-Based Advertising and Ad Delivery and Reporting (§ II(C)(3))

The NAI Code is intended to be technology-neutral, imposing the same obligations on member companies regardless of the technologies they use for Interest-Based Advertising and Ad Delivery and Reporting. At the same time, the NAI believes that all technologies member companies use for online advertising activities should afford users an “appropriate” degree of transparency and control. Accordingly, the NAI has adopted a policy prohibiting member companies from using LSOs for online advertising activities until such time as those technologies allow for an adequate level of insight and control. The NAI continues to believe that Flash and Silverlight do not, at present, provide users with an appropriate level of insight or control and therefore cannot be used for Interest-Based Advertising or Ad Delivery and Reporting purposes consistent with the Code’s requirements. There may, however, be other technologies (aside from standard HTTP cookies) that provide, or can be implemented in such a way, so as to provide an “appropriate” level of transparency and control.²³ Such emerging technologies are particularly important on mobile devices, where cookies are often ineffective. The NAI is working to develop policies with respect to the use of non-cookie technologies, particularly those that facilitate cross-device tracking and those that allow tracking on mobile devices.

Use Limitations (§ II(D))

Children (§ II(D)(1))

This draft revision retains the provision in the current NAI Code forbidding member companies from creating interest segments specifically targeted to children under 13

²³ The requirement that technologies provide “an appropriate degree of transparency and control” applies both to Interest-Based Advertising and to Ad Delivery and Reporting. Because privacy concerns often vary depending on the purpose of the data collection, the degree of transparency and control that is considered “appropriate” may differ depending on the purpose for which the data is collected. For example, data collection for Ad Delivery and Reporting purposes may not require as high of a level of transparency and control as data collection for Interest-Based Advertising. Similarly, the use of a technology that does not offer the transparency of standard HTTP cookies inherent in native browser controls for Interest-Based Advertising purposes may require steps to compensate for that lack of transparency, such as heightened notice requirements.

without obtaining verifiable parental consent. NAI member companies, of course, must also comply with the FTC's COPPA rules as such rules may be updated from time to time.

Prohibited Uses (§ II(D)(2))

Since 2008, the NAI has prohibited the use of OBA segments other than for "Marketing Purposes." With this draft revision, the NAI intends to make clear, for the avoidance of any doubt, that member companies may not use, or allow the use of, such data for eligibility decisions, including employment, health care, and insurance eligibility. These use restrictions apply regardless of whether a user has opted out of Interest-Based Advertising. This revision to the marketing purposes limitations harmonizes with the DAA's Multi-Site Principles by: (1) expanding the prohibition to explicitly include all data collected for Interest-Based Advertising *and* Ad Delivery and Reporting; and (2) spelling out explicitly the purposes that are not permitted for such data. The NAI is not aware of any member companies who have taken a limited view of the "marketing purposes" prohibition in the current NAI Code or who has otherwise sought to use data collected online for eligibility determinations. Nevertheless, the NAI believes that its principles should be as clear as possible with respect to these limitations on data use.

The NAI's prohibition on using Interest-Based Advertising and Ad Delivery and Reporting data other than for marketing is consistent with the White House's "Respect for Context" principle – that consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which the data was provided.²⁴ Consumers are made aware, through in-ad notice and privacy policies of website publishers, that data is collected for the purpose of providing more relevant ads. The use of such data for purposes other than marketing, including any insurance, health, or employment eligibility decisions, would be inconsistent with that context.

Material Changes (§ II(D)(3))

A "material" change for purposes of this provision generally will relate to the collection or use of PII for Interest-Based Advertising purposes or the merger of Non-PII with PII when a company previously represented that it does not collect PII for Interest-Based Advertising purposes or merge PII with Non-PII. Changes are not material for purposes of this provision if they result in less collection or use of data, or when a company changes its

²⁴ See White House Privacy Report, *supra* note 4, at 18 (encouraging companies engaged in online advertising to refrain from collecting, using, or disclosing data that may be used to make decisions regarding employment, credit, and insurance eligibility or similar matters that may have significant adverse consequences to consumers and noting that such uses are at odds with generating revenue and providing consumers with ads that they are more likely to find relevant).

disclosures to provide greater transparency about its existing practices. We encourage member companies to innovate and provide increased transparency around their data collection and use practices, and this section is not intended to cover efforts to provide increased transparency to existing practices.

Transfer Restrictions (§ II(E))

The restrictions on the transfer and use of data collected across non-affiliate websites for Interest-Based Advertising or Ad Delivery and Reporting purposes are extensions of the requirements set forth above for data to be treated as Non-PII rather than PII under the Code. In addition to contractually forbidding the third party from merging the Non-PII collected across non-affiliated websites with PII without obtaining the user's opt-in consent or from otherwise attempting to identify the individual using Non-PII, members should impose technical measures to help prevent the receiving party from engaging in such activities. For example, member companies that pass encrypted data to third parties should not provide the encryption key. These restrictions do not apply when the NAI member is acting as a service provider for a single party and the data transferred is proprietary to that party.

Access (§ II(F)(1))

NAI member companies collect and use data for marketing purposes. Indeed, under the 2008 Code and this draft code, members are forbidden from using, or allowing to be used, the data they collect for any eligibility decisions. Data held solely for marketing purposes does not pose the same risks as data held for purposes such as eligibility determinations, and thus does should not require extraordinary measures to provide users access to such data.²⁵

The 2008 NAI Code requires member companies to provide reasonable access to any PII and associated Non-PII collected and used for Interest-Based Advertising purposes, but *not* requiring companies to provide access to Non-PII that is not associated with PII. The NAI continues to believe that requiring reasonable access to PII and related Non-PII is appropriate, particularly in light of the heightened privacy concerns (and required higher level of choice) involved with the merging of online browsing habits with PII.

Though not required by the NAI Code, some NAI member companies provide users access

²⁵ See FTC Final Privacy Report, *supra* note 4, at 65. Similarly, the White House privacy framework would require “reasonable” access considering the “scale, scope, and sensitivity” of the data collected or maintained and the likelihood that its use may expose consumers to financial, physical, or other material harm.” White House Privacy Report, *supra* note 4, at 19.

to Non-PII-based interest segments associated with their computer or devices. The NAI believes that these “preference managers” are an excellent means of providing users increased levels of transparency and control. Accordingly, the NAI continues to encourage such access to Non-PII as a best practice, but does not believe that providing that access should be a requirement of the NAI Code.

Reliable Sources (§ II(F)(2))

This draft revision refines the “reliable sources” requirement in the current NAI Code to specifically require members to conduct appropriate due diligence to ensure that they obtain data used for Interest-Based Advertising and Ad Delivery and Reporting from reliable sources that provide users with appropriate levels of notice and choice. Generally, the NAI encourages member companies to obtain data from companies that are part of the NAI or another self-regulatory program. Additional steps that companies should take to ensure that their data sources provide appropriate protection for data include: (1) reviewing the company’s privacy policy; (2) understanding the technologies the company uses to collect data and whether the company provides an Opt-Out Mechanism that is effective with respect to those technologies and that, if possible, is included on an industry-wide opt out page; (3) ensuring that the data source secures an appropriate level of consent; and (4) reviewing the company’s marketing materials to understand how the company collects data from users and what types of data it collects. Such measures are particularly important when member companies obtain data from companies that are not NAI members or otherwise subject to oversight of their privacy practices.

Data Retention (§ II(F)(4))

This draft language, like the NAI’s current data retention requirement, requires member companies to keep data that is “linkable to a device,” and thus considered Non-PII under the Code (or any PII used for Interest-Based Advertising or Ad Delivery and Reporting purposes) only so long as necessary to serve their business needs. In accordance with section II(B)(1)(f), member companies are required to publicly disclose the period for which they retain such data for those purposes. At the end of that publicly stated retention period, members are required to either delete such data, or to render it De-Identified Data by taking steps to ensure that it cannot reasonably be linked to a particular person, computer, or device. Such measures may include removing unique user identifiers, removing IP addresses, and/or deleting the last four digits of IP addresses.

In its recent Privacy Report, the FTC urged self-regulatory organizations like the NAI to provide further guidance to organizations concerning appropriate retention periods.²⁶ NAI staff regularly provides such guidance to companies in the course of its member on-

²⁶ See FTC Final Privacy Report, *supra* note 4, at 28-29.

boarding procedures and annual compliance reviews, urging companies to limit the retention of data to the extent necessary based on the particular business practices of each company. The NAI believes that an even more effective method of limiting retention periods is to require members to disclose those retention periods. Such transparency provides companies an incentive to carefully examine their practices and ensure that they do not keep data longer than necessary to serve their business needs.