2015 UPDATE TO THE NAI Code of Conduct

June 2017

NAI
Network Advertising Initiative

INTRODUCTION

The Network Advertising Initiative (NAI) is the leading non-profit, self-regulatory body governing advertising technology providers in the online advertising ecosystem. Created by the online advertising industry in 2000, the NAI is one of the Internet's longest standing, and most respected, industry self-regulation efforts. The organization is currently composed of nearly 100 member companies and is expanding.

For nearly 15 years, 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 Interest-Based Advertising and related practices. These standards are set forth in the NAI Self-Regulatory Code of Conduct (referred to as the Code) which was first adopted in 2000 with the unanimous support and praise of the U.S. Federal Trade Commission (FTC).

The Code imposes notice, choice, accountability, data security, and use limitation requirements on NAI member companies. 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, members are held to their promise to adhere to the Code.

The Code is periodically reviewed and updated in an effort to anticipate and respond to practical questions, rapidly evolving technologies and business models, and new issues raised by policymakers. Consequently, the Code was revised in 2008 and 2013. This 2015 update is designed to clarify aspects of the 2013 Code of Conduct.

Purpose of this Updated Code

The 2013 Code of Conduct significantly revised and updated the NAI's self-regulatory framework. This 2015 update intends to clarify certain obligations present in the 2013 Code of Conduct and the accompanying commentary in response to questions received by the NAI, rather than add new substantive requirements for member companies. For example, this Code clarifies that the practice of Retargeting currently carries the same obligations and requirements under the Code as Interest-Based Advertising (IBA). In addition, the Code explains that members' "Interest-Based Advertising" activities based on sensitive health conditions or treatments require "Opt-In Consent." Although these interpretations were discussed in the commentary to the 2013 Code of Conduct, they have been moved directly into the text of the Code in this 2015 update for additional clarity and emphasis that NAI staff views them as Code requirements.

Scope of the Code

The Code governs only NAI member companies. It does not govern all data collection by member companies. Rather, it is limited to members' "Interest-Based Advertising" and "Ad Delivery and Reporting" activities, as defined in the Code. To the extent a member company collects data across non-affiliated websites on a browser for the purpose of either delivering advertising or providing advertising-related services across multiple websites, that activity is governed by the Code. Similarly, selecting an advertisement to serve a user on one website based on a user's activity on one or more different, unaffiliated websites, would also be an activity governed by the Code.

The Code applies to members' Interest-Based Advertising and Ad Delivery and Reporting Activities that: (1) occur in the United States or (2) apply to U.S. users. The NAI encourages its members to apply the high standards of the 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 all laws applicable to their businesses. The Code generally goes above the requirements of applicable laws. However, to the extent there is a conflict between the Code and a member's obligations under applicable law, the member shall abide by the applicable law.

The Code does *not* govern member companies' activities insofar as they are acting as first parties or solely on behalf of a single first party. For example, collection and use by a member company of data on a single domain, or set of affiliated domains, for the purpose of conducting analytics, are not be covered by the Code.

Member companies may use various technologies to engage in Interest-Based Advertising as business models expand beyond traditional desktop web browsing to mobile devices and tablets.[1] The Code is intended to be technology-neutral, imposing obligations on members' Interest-Based Advertising activities regardless of the technologies they use.

The NAI continues to believe that these technologies, when used by members for Interest-Based Advertising, should provide users with an appropriate degree of transparency and control consistent with the Code requirements.

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

In 2010, the NAI joined the Digital Advertising Alliance (DAA). The DAA 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 Online Behavioral Advertising (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, internet service providers, cell phone carriers, social networks, advertisers, offline data providers, *and* the digital technology companies 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 ad tech companies such as networks and platforms, but also on website publishers and brand advertisers.

1 This update to the Code is not intended to govern member companies' collection and use of data through mobile applications. Instead, the Code served as the baseline standard from which the Mobile Application Code was developed. The Mobile Application Code provides guidelines for members that specify the notice, choice, and other protections required of member companies collecting and using data through mobile applications. The Mobile Application Code is available at http://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf.

2 *See* Digital Advertising Alliance, Self-Regulatory Principles for Online Behavioral Advertising (DAA OBA Principles), available *at* http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; *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.

The Code largely harmonizes with the DAA's Principles as they apply to the OBA and Ad Delivery and Ad Reporting by NAI member companies. Thus, for example, the Code imposes an "enhanced" notice requirement for ads informed by Interest-Based Advertising data. Similarly, the Code also makes explicit the purposes for which member companies may not use, or allow the use of, data collected for advertising purposes. Importantly, the requirements for the provision of opt-out choice under the DAA's Multi-Site Data Principles generally mirror the NAI's requirements for opt-out choice under the NAI Code.

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 contained in the DAA Principles that are not applicable to third-party advertising companies in the advertising ecosystem are not included in the NAI Code. Similarly, obligations imposed on third-party advertising companies are in some cases phrased differently in this Code than in the DAA Principles.

Framework of the Code

The fundamental principle underpinning the 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's Final Privacy Report and the White House Privacy Report.[4] Both of these reports explicitly acknowledge that privacy protections should not be applied in a "one-size fits all" approach. Instead, privacy safeguards should be flexible, scalable, and take into account the context in which the data is collected and used.

To that end, this Code identifies three categories of data with varying levels of "identifiability" and imposes different obligations on NAI members based on the sensitivity of the data. These three categories are:

1) 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 is linked or reasonably linkable to a particular *computer or device*; and De-Identified Data refers to data that is not linkable to either an individual or a device. In addition, this Code imposes obligations with respect to "Sensitive Data" and "Precise Location Data" use for Interest-Based Advertising. Sensitive Data is defined to include specific types of PII that are sensitive in nature, as well as Non-PII related to sensitive health or medical conditions and sexual orientation.

---

3 The NAI Code does not impose any direct obligations on non-NAI companies, but does promote actions by NAI members companies to increase trust in the ecosystem. For instance, members have an obligation to work with reliable sources and to take steps to require those websites with which they have a contract and engage in Interest-Based Advertising to post notice regarding the Interest-Based Advertising activity. However, the Code does not impose direct obligations on non-NAI member companies and the NAI compliance program does not review the practices of non-members.

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.

NAI Oversight and Monitoring

The NAI Code is a self-regulatory code. The NAI recognizes that the application of the Code may involve subjective judgments and that technical, operational and policy questions may affect such judgments. For that reason, as a self-regulatory body, it is the intent that the NAI is the final arbiter of how the Code applies to its members' practices in any given instance. Only the NAI staff is authorized to interpret the requirements of the Code and to evaluate compliance with and enforce violations of the Code. If NAI staff determines that there is an instance of non-compliance with the Code by a member, and if a member refuses to implement the recommended steps to bring its practices into compliance, the NAI enforcement procedures allow NAI to refer the matter to the FTC. In making such a referral, NAI does not ask the FTC to interpret its Code, but simply to address the member's failure to comply with NAI's interpretation and application of the Code.

2015 UPDATE TO THE 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 data 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. RETARGETING

Retargeting is the practice of collecting data about a user's activity on one web domain for the purpose of delivering an advertisement based on that data on a different, unaffiliated web domain. Although it is a separate and distinct practice from Interest-Based Advertising, unless specified otherwise, requirements and obligations set forth under the Code for Interest-Based Advertising apply equally to Retargeting.

D. 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.

E. NON-PII

Non-PII is data 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' computers or devices and IP addresses, where such identifiers or IP addresses are not linked to PII. Non-PII does not include De-Identified Data.

F. 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.

G. PRECISE LOCATION DATA

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

H. SENSITIVE DATA

Sensitive Data includes:

- Social Security Numbers or other government-issued identifiers;
- Insurance plan numbers;
- Financial account numbers;
- Information about any past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history, based on, obtained, or derived from pharmaceutical prescriptions or medical records, or similar health or medical sources that provide actual knowledge of a condition or treatment (the source is sensitive);
- Information, including inferences, about sensitive health or medical conditions or treatments, including, but not limited to, all types of cancer, mental health-related conditions, and sexually transmitted diseases (the condition or treatment is sensitive regardless of the source); and
- Sexual orientation.

I. OPT-IN CONSENT

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

J. OPT-OUT MECHANISM

An Opt-Out Mechanism is an easy-to-use mechanism by which individuals 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 user choice mechanisms.

2. Members should use reasonable efforts to educate individuals about Interest-Based Advertising and the choices available to them with respect to Interest-Based Advertising.

B. TRANSPARENCY AND NOTICE

1. Each member company 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 a general description of the following, as applicable:

    a. The Interest-Based Advertising, and Ad Delivery and Reporting activities undertaken by the member company;

    b. The types of data collected or used for Interest-Based Advertising purposes, and Ad Delivery and Reporting purposes, including any PII;

    c. How such data will be used, including transfer, if any, to a third party;

    d. The technologies used by the member company for Interest-Based Advertising, and Ad Delivery and Reporting; and

e. The approximate length of time that Interest-Based Advertising or Ad Delivery and Reporting data will be retained by the member company.

f. A statement that the company is a member of the NAI and adheres to the Code; and

g. A link to an Opt-Out Mechanism for Interest-Based Advertising.

2. Members that use standard interest segments for Interest-Based Advertising purposes that are based on health-related information or interests shall disclose such segments on their websites.

3. Members shall take steps to require those websites with which they have a contract and engage in Interest-Based Advertising to clearly and conspicuously post notice, which contains:

   a. A statement of the fact that data may be collected for Interest-Based Advertising purposes on the website;

   b. A description of the types of data that are collected for Interest-Based Advertising purposes on the website;

   c. An explanation of the purposes for which data is collected by, or will be transferred to, third parties; and

   d. A conspicuous link to an Opt-Out Mechanism for Interest-Based Advertising.

4. As part of members' overall efforts to promote transparency in the marketplace, members should make reasonable efforts to confirm that websites where the member collects data for Interest-Based Advertising purposes furnish notices comparable to those described in II.B.3 above.

5. Members shall provide, or support the provision or implementation 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, unless notice is otherwise provided on the page where the ad is served outside of the publisher's privacy policy or terms of service.

C. USER 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 purposes shall require 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 user's Opt-In Consent.

d. Use of Precise Location Data for Interest-Based Advertising purposes shall require a user's Opt-In Consent.

e. Use of Sensitive Data for Interest-Based Advertising purposes shall require a user's Opt-In Consent.

2. When a user has opted out of Interest-Based Advertising from a particular member or members, those member companies must honor the user's choice as to the particular browser. Member companies may continue to collect data for other purposes, including Ad Delivery and Reporting. However, any data collected by a member company while a browser is opted out may not be used for Interest-Based Advertising purposes, regardless of the future opt-out status of the browser and regardless of the technology or technologies used for Interest-Based Advertising by the member company, absent Opt-In Consent.

3. The technologies that members use for Interest-Based Advertising purposes must provide users with an appropriate degree of transparency and control.

D. USE LIMITATIONS

1. Member companies shall not create Interest-Based Advertising segments specifically targeting children under 13 without obtaining verifiable parental consent.

2. Members shall not use, or allow the use of, Interest-Based Advertising or Ad Delivery and Reporting data for any of the following purposes:

   a. Employment Eligibility;

   b. Credit Eligibility;

   c. Health Care Eligibility; or

   d. Insurance Eligibility and Underwriting and Pricing.

3. Members who make a material change to their policies and practices around Interest-Based Advertising 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 the provisions of this Code concerning PII.

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 for Interest-Based Advertising purposes without obtaining the individual's Opt-In Consent. This requirement does not apply if the Non-PII is proprietary data of the receiving party.

F. DATA ACCESS, QUALITY, SECURITY, AND RETENTION

1. Members shall provide users with reasonable access to PII, and other information that is associated with PII, retained by the member for Interest-Based Advertising purposes.

2. Members shall conduct appropriate due diligence to help ensure that they obtain data used for Interest-Based Advertising purposes 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 purposes and/or Ad Delivery and Reporting purposes 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. The Code is self-regulatory in nature but is binding on all members of the NAI.

2. To help ensure compliance with the Code, each member company should designate at least one individual with responsibility for managing the member's compliance with the Code and providing training to relevant staff within the company.

3. Membership in the NAI requires public representations that a member company's business practices adhere to the Code as it applies to its business model, as supplemented by applicable implementation guidelines that may be adopted by the NAI Board from time to time. Such representations involve explicit acknowledgement of NAI membership and adherence to the Code in each member's publicly available privacy notice, and inclusion in a membership listing of participating NAI 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 Code by NAI compliance staff or other NAI designees. Members shall fully cooperate with NAI compliance staff or NAI designees, including in the course of annual compliance reviews and any investigation of a potential violation of the Code.

2. The NAI's policies and procedures for annual compliance reviews and compliance investigations may be updated from time to time. 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 FTC. These policies and procedures, including any updates or revisions, shall be made available on the NAI website.

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. USER COMPLAINTS

1. The NAI website shall include a centralized mechanism to receive an individual's questions or complaints relating to members' compliance with this Code.

2. Each member shall provide a mechanism by which individuals can submit questions or concerns about the company's collection and use of data for Interest-Based Advertising purposes, and shall make reasonable efforts to timely respond to and resolve questions and concerns that implicate the member company's compliance with the Code and NAI policies.

COMMENTARY TO 2015 UPDATE TO THE NAI CODE OF CONDUCT

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. Instead, the commentary's purpose is to explain the intent behind certain provisions of the Code. The commentary is also intended to provide examples of possible measures member companies may take to meet the substantive obligations of the Code.

I. Definitions

INTEREST-BASED ADVERTISING AND RETARGETING

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 known or inferred from the data collected.[5] The FTC maintains the view that to treat domains as owned or operated by the same entity, their corporate affiliation must be made clear to users by those entities.[6] Further, Interest-Based Advertising has 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."

Consistent with the FTC's definition of "online behavioral advertising," and DAA's OBA Principles, the definition of Interest-Based Advertising does *not* include "contextual advertising." Contextual advertising means the ads are selected depending solely upon the content of the page on which it is served. Contextual advertising also covers "first party" marketing, in which ads are customized or products are suggested based on the content of the site that the user is visiting at that time (including the content viewed, the searches performed, or the user's location when viewing the page).[7] Those activities are outside the scope of the Code.

The Code defines Retargeting as the practice of collecting data about a user's activity on a single web domain for the purpose of delivering an advertisement based on that data on a different, unaffiliated web domain. An example of Retargeting is the delivery of an advertisement for a product or service that a user previously viewed on an unrelated web domain, without necessarily placing that user in an interest segment. The NAI recognizes that Retargeting is a separate and distinct business practice from Interest-Based Advertising because the advertisement may be selected based on activity on a single web domain and the user may not necessarily be included in an interest segment based on activity on multiple web domains. However, consistent with prior versions of the Code, at this time Code requirements and obligations for Interest-Based Advertising apply equally to Retargeting.[8]

---

5 Certain practices, such as the provisioning of offline data for use in targeted online advertising, are not directly covered by this Code. Some member companies have committed to applying NAI principles to these practices in order to further promote consumer privacy. NAI will enforce the relevant NAI Code provisions on such members. NAI will apply any future updates to the Code that cover provisioning of offline data for use in targeted advertising to all NAI members.

6 *See* FTC Final Privacy Report, *supra* note 5, at 42.

7 *See* FTC Final Privacy Report, *supra* note 5, at 41; DAA OBA Principles, *supra* note 3, at 10-11 (defining OBA to exclude first party activity, ad delivery and ad reporting, and contextual advertising).

8 The DAA Online Interest-Based Advertising Accountability Program has also indicated that it considers Retargeting to be covered by the DAA Self-Regulatory Principles for Online Behavioral Advertising (DAA OBA Principles). *See* http://www.bbb.org/us/storage/113/Documents/23andMe-Decision-20131115.pdf.

PII, NON-PII, AND DE-IDENTIFIED DATA

As stated in the introduction to the Code, the Code divides data into three categories of "identifiability": PII, Non-PII, and De-Identified Data.

The key distinction between the three categories is the type of identifier that the data is linked to:

- Data that is used or intended to be used to identify an *individual* is considered PII.
- Data that is linked or reasonably linkable to a specific *computer or device* is considered Non-PII.
- Data that is not linked or reasonably linkable to either an individual or to a specific computer or device is considered De-Identified Data.

This framework generally mirrors the "reasonable linkability" analysis set forth in the FTC Final Privacy Report. The Report rejects a "bright line" test and instead adopts a scaled approach to evaluating risks and determining the obligations that attach to data.[9] This scaled approach recognizes that different categories of data present different levels of risk, a concept likewise reflected in the NAI Code. Although some regulators have raised questions about the utility of maintaining the traditional distinctions between PII and Non-PII,[10] the NAI believes that it is appropriate for the Code to continue to discourage members from linking the Non-PII they collect for Interest-Based Advertising and Ad Delivery and Reporting purposes with particular individuals for Interest-Based Advertising. To encourage these data minimization efforts, the 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.[11]

PII

PII includes 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. In addition to the examples of PII enumerated in the definition, PII could include data derived from 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 a unique individual, even if such faceprints were not linked to name, address, telephone number, email address, or other traditional identifiers.

The Code requirements that apply to PII equally apply to any data or data sets tied to PII. For example, if demographic information (e.g., age, gender), which would typically be considered Non-PII on its own, is attached to a name or email address, it would be treated as PII under the Code as a result of being attached to the aforementioned PII. Similarly, a cookie identifier which would otherwise qualify as Non-PII under the NAI Code, would be treated as PII if such an identifier is tied to PII, such as a name or email address.

Non-PII

Non-PII is defined as "data 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' computers or devices and IP addresses, where such identifiers or IP addresses are not linked to PII. Non-PII does not include De-Identified Data.

---

9 *See* FTC Final Privacy Report, *supra* note 5, 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).

10 *See id.* at 18-19.

11 The NAI remains focused on the substantive differences between the three categories of data defined in the Code, more so than on the labels themselves. As the ecosystem evolves, however, NAI may revise the labels, names, and definitions of different categories of data in future iterations of the Code.

Examples of how a member company may help ensure that the data it collects and uses for Interest-Based Advertising purposes meets this standard may be to: (1) take measures to help ensure that the data it collects or receives cannot reasonably be linked to a particular individual, such as using only randomly generated numeric identifiers rather than names or other personal information; (2) publicly commit to maintain the data as Non-PII; and/or (3) take reasonable steps, such as contractual measures, to prevent 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) for Interest-Based Advertising purposes.

De-Identified Data

The Code defines De-Identified Data as "data that is not linked, or reasonably linkable to an individual or to a particular computer or device." Data would be considered "De-Identified Data" under the NAI Code if a member were to take steps similar to those enumerated above with respect to Non-PII, such as: (1) taking 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 the unique user identifiers (*e.g.,* cookie identifier) or IP addresses, or truncating the IP addresses; (2) publicly committing to maintain and use the data in a de-identified fashion and not attempting to re-associate the data with an individual or with a particular computer or device; (3) obtaining satisfactory 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 Data Principles.[12]

Under the definition of De-Identified Data, the NAI Code refers to both group data and certain individual data. First, De-Identified Data includes what is commonly referred to as group or aggregate data, such as monthly aggregate reports on an advertising campaign provided by members to their clients. Aggregate data, or cross-sectional data, does not contain individual-level or device-level information that can be tied back to a specific individual or device. For example, the overall conversion rate for a campaign among young men in a specific state is considered De-Identified Data.

Second, De-Identified Data covers data that was once linked to an individual or device, which has then gone through a process that reasonably removes the links to any specific individual or device. For example, a member can remove or truncate identifiers (e.g., cookie identifiers or IP addresses) so that the data will reflect that a unique browser visited certain websites, but the data will no longer be associated with a particular browser.

PRECISE LOCATION DATA

The definition of "Precise Location Data" is meant to recognize that a range of technologies available today or in the future may be able to provide members, "with reasonable specificity," the actual physical location of an individual.

Accordingly, the definition Precise Location Data is intended to *exclude* more general location data, such as postal code, city, or neighborhood whether that location data is derived from an IP address or other sources.[13]

The definition of Precise Location Data also does not include location data that has been altered, or will be altered, upon its provision for use in Interest-Based Advertising, so that a member is unable to determine with reasonable specificity the actual physical location of an individual or device. For example, a member will not

12 *See* DAA Multi-Site Data Principles, *supra* note 3, at 8.

13 These examples are provided in this Code for illustrative purposes only.

be deemed to be using Precise Location Data as defined by the Code if the member removes a sufficient number of decimals from a device's latitude/longitude coordinates from the location data it receives before using the data for Interest-Based Advertising. Similarly, Precise Location Data only includes information that describes an actual physical location. As such, if a member converts a precise location (e.g. a specific coffee shop at a specific street address) to a general category (e.g. coffee shop), the resulting information is not covered by the definition of Precise Location Data.

In addition, consistent with the scope of Interest-Based Advertising, the Code requirements for the use of Precise Location Data do not apply when a member company does not store or otherwise save the Precise Location Data after serving or delivering an advertisement in real-time.

SENSITIVE DATA

Health

The 2015 Update to the Code of Conduct clarifies that the definition of "Sensitive Data" includes two categories of data: (1) data about a health condition or treatment derived from a sensitive source and (2) data about certain sensitive conditions regardless of the source of the data. The collection and use of Sensitive Data for Interest-Based Advertising requires Opt-In Consent from individuals.

First, Sensitive Data includes information about any past, present or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history, based on, obtained or derived from a patient's medical records, pharmaceutical prescriptions or similar sources from a health care provider that impart actual knowledge of a condition or treatment. It is the use of information based on actual knowledge of a health or medical condition or treatment from a patient's medical records for Interest-Based Advertising that triggers the requirement for Opt-In Consent, regardless of which health or medical condition the segment references.

Second, this update to the Code also clarifies that Interest-Based Advertising (whether through "standard" interest segments, custom segments, or Retargeting) based on an inferred interest in sensitive health conditions requires a user's Opt-In Consent. It is often difficult to draw bright lines between "sensitive" and "non-sensitive" data in the health space because whether a particular condition is considered sensitive may depend on the affected individual and a number of subjective considerations.

In recognition of this subjectivity, and following questions and commentary provided in response to prior drafts of the Code, the NAI has not developed an exhaustive list of conditions or treatments that it considers to be "sensitive." Rather, the NAI provides its member companies with a number of factors to consider when determining whether a particular condition or treatment is "sensitive."[14] The factors include: the seriousness of the condition, how narrowly the condition is defined, its prevalence, whether it is something that an average person would consider to be particularly private in nature, 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, sensitive health segments, which require Opt-In Consent under the Code, include, but are not limited to, categories such as: drug addiction, all sexually transmitted diseases (such as AIDS, HIV, HPV), all types of mental health conditions (such as generalized anxiety disorder, schizophrenia, Alzheimer's, depression, anorexia/bulimia), pregnancy termination, as well as cancer. In contrast, the NAI considers many

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

conditions such as acne, allergies, dental, vision, heartburn, cold and flu, sinus, headache, back pain, first aid, sore throat, and cholesterol management, to be generic and not topics that require Opt-In Consent. Similarly, interest in diet, nutrition, exercise, beauty, hair removal, health and fitness, as well as vitamins and supplements, typically do not qualify as "sensitive" under the Code, and thus do not require Opt-In Consent. Finally, more general segments such as men's health, women's health, senior health needs, or children's health also do not meet the criteria for Opt-In Consent under the Code.

The NAI acknowledges that these are subjective considerations and that no one factor is determinative. Therefore, any member company that conducts a reasonable analysis of a health condition and determines that it does not meet the factors of a sensitive health segment will not be in violation of the Code even if other stakeholders, including, but not limited to, the NAI compliance team, arrive at a different conclusion. However, a member may be asked to change its practice with respect to Interest-Based Advertising involving a sensitive health condition that NAI staff determines meets the criteria outlined here, subject to all procedure and rights of appeal under the NAI Sanction Procedures.

As with any subjective category, there will be certain conditions that do not clearly fall on either side of the line of sensitive. For that reason, the NAI Code also requires members to publicly disclose any standard interest segments they use for Interest-Based Advertising that are related to health conditions or treatments, even if those segments are not precise or sensitive (see the discussion of Health Transparency obligation, below).

Sexual Orientation

The Code prohibits companies from collecting or storing information about an individual's status or perceived status as gay, lesbian, bisexual, or transgendered for Interest-Based Advertising without obtaining Opt-In Consent. The Code does *not* intend to prohibit Retargeting based on visits to dating websites, wedding registries, services for couples (such as travel), or similar content. The intent of the Code is to prohibit the creation of interest segments such as "gay male" or "interested in LGBT issues," as well as the Retargeting of visitors to sites that reflect the individual's sexual orientation, such as dating or travel sites targeted to LGBT visitors. While advertising on such websites and to the LGBT community is valuable, this policy recognizes that LGBT status may be considered sensitive in some contexts, and thus that Opt-In Consent shall be obtained before using such data for Interest-Based Advertising.

II. Member Requirements

MEMBER-PROVIDED NOTICE (§ II.B.1)

Section II.B.1 of the NAI Code requires companies to provide clear, meaningful, and prominent notice concerning their data collection practices. This requirement is not limited to Interest-Based Advertising, and applies equally to Ad Delivery and Reporting. Some steps that members can take to ensure that their notice is "prominent" is to provide conspicuous links to their consumer-facing disclosures, such as obvious links to privacy policies, as well as "consumer information" links, and/or 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 appropriately sized 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 member company's data collection and use practices in an understandable manner. The notice should also accurately reflect the member company's data collection and use practices. Members that obtain data from third parties for

purposes of supplementing user profiles should disclose such data collection and how the data is used for Interest-Based Advertising purposes.

Members should also describe their data collection and use practices in as clear and concise a manner as possible. Members are also required to disclose the technologies they use for Interest-Based Advertising and Ad Delivery and Reporting. Member companies are *not* required to disclose the technologies they use with a level of specificity that would reveal their proprietary business models.

NAI recognizes that members face conflicting views regarding what to include in privacy policies. They must balance the pressure to provide more detailed disclosures with countervailing pressures for simplified privacy statements that are concise and readable. NAI recognizes that it is important to strike this balance. Consequently, it is the NAI's position that a member's notice should generally disclose its data collection, use, and retention practices. The Code sets forth the disclosures the NAI expects in a member's privacy policy or privacy disclosure. Additionally, during annual compliance reviews, or at a member's request, NAI staff evaluates the member's privacy policy to help ensure that it complies with Code requirements and may recommend best practices consistent with the Code.

HEALTH TRANSPARENCY REQUIREMENT (§ II.B.2)

The health transparency requirement is intended to capture those interest segments for which Opt-In Consent is not required under Section II.C.1.e of 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. For example, member companies may seek to target users on the basis of general health categories such as headaches, allergies, or diet and fitness that would not amount to sensitive data that requires Opt-In Consent. Nonetheless, the use of such standard segments would require disclosure under the transparency requirements. 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 a list of any 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 use standard interest segments, but may engage in Retargeting or the creation of "custom" segments. In such cases, members should instead disclose a representative sample of their health-related custom segments and Retargeting activities, or otherwise explain their use of health-related information for Interest-Based Advertising and Retargeting.

WEBSITE NOTICE (§ II.B.3-5)

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

If an NAI member company has a direct contractual relationship with a website where it conducts Interest-Based Advertising, it shall take steps to contractually require the website to post notice of Interest-Based Advertising and a link to an Opt-Out Mechanism.[15] The steps may comprise the inclusion of these requirements in contracts, terms of service, and insertion orders, as well as negotiation with partners to help ensure that such notice is provided even in the absence of contractual requirements. The notice should be provided in a privacy policy or separate footer link, such as "About our Ads."

15 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 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.

Members should use reasonable efforts to enforce contractual notice provisions, and to evaluate whether notice is provided even in the absence of a contractual requirement to provide such notice. Members should seek to ensure that notice is provided where they collect data. For example, members may regularly check a reasonably-sized sample of the websites where they conduct Interest-Based Advertising to ensure that the websites provide appropriate notice, following up with those that do not.[16]

Enhanced Notice Requirement (§ II.B.5)

The Code requires members to "provide, or support the provision or implementation of" notice in or around the ads they serve. The NAI expects that members 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. For instance, some members do not collect data but facilitate the collection of data by their clients for Interest-Based Advertising through their platform. These members may provide their clients with the ability to include this notice on their advertisements through platform settings. Notice in or around an advertisement is not necessary if the notice of Interest-Based Advertising is provided outside of the privacy policy or the terms of service of a webpage where the advertisement is served.

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. Finally, the NAI will work with DAA and DAA member organizations to educate advertisers and publishers on the requirements of the DAA program.

USER CONTROL (§ II.C)

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

The Code requires members to provide an Opt-Out Mechanism for opting out of the collection and use of Non-PII for Interest-Based Advertising purposes. The Code also requires that members obtain Opt-In Consent for the collection and use of Sensitive Data and Precise Location Data for Interest-Based Advertising. Members must also obtain Opt-In Consent for the retrospective merger[17] of PII and Non-PII for Interest-Based Advertising purposes. For the prospective merger of PII and Non-PII for Interest-Based Advertising purposes, the Code requires the provision of an Opt-Out Mechanism coupled with "robust" notice. To be considered "robust" under this provision, the 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.

16 The contractual notice provisions are intended to help 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 that provide in-ad notice pursuant to Section II.B.5 and only collect data for Interest-Based Advertising purposes 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.

17 For the purpose of this Code, "retrospective merger" is the combination of PII with previously collected Non-PII by a member. This could include the merger of existing segment information with a newly collected name or email address. Meaning, the individual did not have the expectation that when the individual's Non-PII was originally collected that it would later be tied to their PII. "Prospective merger" is the combination of PII with Non-PII to be collected on a going-forward basis by a member. The Non-PII was collected by the member before the PII was collected. An example of this could include the collection of potential purchase intent by a member in combination with a name or email address that had already been provided by the user.

Honoring Opt-Out Choices (§ II.C.2)

Following an opt-out, member companies must cease collecting and using data for Interest-Based Advertising purposes for that browser.[18] Member companies may, however, continue to collect data for other purposes, such as Ad Delivery and Reporting. Any data collected while a browser is opted out may not be used for Interest-Based Advertising purposes, regardless of the future opt-out status of the browser, or the technology used for Interest-Based Advertising. For example, a user opts out of Interest-Based Advertising on her browser, but a month later deletes the opt out cookie. Any data collected by the member company on the opted out browser during the month the browser was opted out may not be used for Interest-Based Advertising, even after the opt-out choice is deleted. Of course, a user may always choose to have such data used for Interest-Based Advertising by providing the member company with express, affirmative consent.

Further, if an opt-out cookie is set on a browser, members must cease the collection and use of data for Interest-Based Advertising purposes not only with cookies, but also with any other technology used by the member for Interest-Based Advertising on that browser. Similarly, any data collected while a browser is opted out, regardless of the member's Interest-Based Advertising technology, may not be used for Interest-Based Advertising purposes.

While members 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 users 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 Mechanism, at a minimum, results in the cessation of Interest-Based Advertising for the applicable browser. While the NAI is working to expand the scope of its Code, some responsible actors, with business models that are related to Interest-Based Advertising, have voluntarily gone through the NAI compliance review process and have agreed to honor and apply NAI standards even to practices that do not fall squarely under the Code. In such cases, the NAI expects a member's opt-out to be consistent with the representations made to NAI staff and will hold members accountable for their representations through the NAI's sanction procedures even if the opt-out may otherwise comply with NAI Code requirements.

Technologies Used for Interest-Based Advertising (§ II.C.3)

The NAI recognizes that new business models are in development and that technologies are evolving rapidly. As part of that process, NAI seeks to ensure that, with their inevitable adoption in the marketplace, new business models and technologies are implemented by NAI members in a manner that is consistent with the core requirements of the NAI Code and the spirit of the Fair Information Practice Principles. The NAI intends to remain technology-neutral while helping to ensure the overall health of the digital advertising ecosystem. As such, the NAI has formed a Beyond Cookies Working Group with a goal to finalize guidance for the use of non-cookie technologies in 2015.

As NAI members develop new business models utilizing non-cookie technology, NAI urges that they seek to implement these business models with the principles of the NAI Code in mind. NAI will be transparent about the evolution of its guidance on non-cookie technology for Interest-Based Advertising with all members, as well as regulators, policy makers, and other interested stakeholders. NAI strives to ensure an efficient process to update its Code and guidance in order to produce a practical, scalable, and implementable standard that adapts responsible data collection and use principles central to the NAI Code to these new technologies.

18 Certain browsers may enable separate user profiles, with independent cookie or local storage caches. In such cases the browser may only permit member companies to set and read preferences for the profile in use. Accordingly, a member must honor the opt-out for the profile that expressed the choice.

USE LIMITATIONS (§ II.D)

Children (§ II.D.1)

The Code prohibits member companies from creating segments for Interest-Based Advertising specifically targeted to children under 13 without obtaining verifiable parental consent. NAI member companies must also comply with the FTC's Children's Online Privacy Protection Act (COPPA) rules, as such rules may be updated from time to time.

Prohibited Uses (§ II.D.2)

The NAI's prohibition of the use of data collected for Interest-Based Advertising and Ad Delivery and Reporting for eligibility decisions is consistent with the White House's "Respect for Context" principle. This principle states 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.[19] Users 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, credit, or employment eligibility decisions, would be inconsistent with that context.

Material Changes (§ II.D.3)

Generally, a "material" change for purposes of this provision will relate to the collection or use of PII for Interest-Based Advertising purposes or the merger of Non-PII with PII when a member previously represented that it does engage in these activities. Under the Code, changes are not considered "material" for the purposes of this provision if they result in less collection or use of data, or when a company changes its disclosures to provide greater transparency about its existing practices. NAI encourages its members to innovate and provide increased transparency around their data collection and use practices.

TRANSFER RESTRICTIONS (§ II.E)

The Code places limitations on the transfer of data collected across non-affiliate websites for Interest-Based Advertising purposes to unaffiliated third parties. These are extensions of the requirements set forth above for data to be treated as Non-PII rather than PII under the Code. For instance, under the Code, members maintain the Non-PII status of data by contractually requiring that all parties to whom they provide Non-PII collected across web domains owned or operated by different entities not attempt, for Interest-Based Advertising purposes, to merge such Non-PII with PII held by the receiving party without obtaining the individual's Opt-In Consent (unless the Non-PII is proprietary to the receiving party). Members can also impose technical measures to help prevent the receiving party from engaging in such activities. For example, members that pass user-level data to third parties may encrypt potential identifiers to prevent impermissible uses by the recipients. 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. But members are prohibited from using, or allowing to be used, the data they collect for any eligibility decisions. To foster transparency and control where PII is associated with Non-PII, the Code requires member companies to provide reasonable access to any PII and associated Non-PII collected and used for Interest-Based Advertising purposes. However, the Code does *not* require companies to provide access to Non-PII that is not associated with PII.

---

19 *See* White House Privacy Report, *supra* note 5, 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).

Though not required by the Code, some NAI member companies provide users access to Non-PII-based interest segments associated with their browsers. The NAI believes that these "preference managers" are an excellent means of providing users with increased levels of transparency and control. Accordingly, the NAI continues to encourage members to provide such access to Non-PII when practicable.

RELIABLE SOURCES (§ II.F.2)

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 members may take to help ensure that their data sources provide appropriate notice and choice to users include: (1) confirming that the data source is entitled to acquire, provide and/or license the data to the member; (2) reviewing the data source's privacy policy (if applicable); (3) understanding the technologies the data source uses to collect data and whether the company provides an effective Opt-Out Mechanism (if applicable) that, if possible, is included on an industry-wide opt-out page; (4) taking reasonable steps to evaluate whether the data source secures an appropriate level of consent from users for the types of data it collects, which may be accomplished by reviewing the data source's privacy policy, commercial agreements, and marketing materials for information on how the company collects data. 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 SECURITY (§ II.F.3)

Members are required to attest in writing that they have reasonable and appropriate procedures in place to secure their data as required by the NAI Code. NAI staff does not conduct security audits of member companies or otherwise review the data security practices of members. NAI staff does not opine on or otherwise advise members on specific data security measures, as what is reasonable and appropriate depends on the members' business models. Because business models vary from member to member, member companies, not NAI staff, are in the better position to determine what is appropriate under a given set of circumstances.

DATA RETENTION (§ II.F.4)

The NAI Code requires member companies to keep data that is "reasonably 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 is 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 individual, computer, or device.

509 7th Street, NW
Washington, DC 20004

www.networkadvertising.org

NAI
Network Advertising Initiative