



2018

NAI Code of Conduct

INTRODUCTION

The Network Advertising Initiative (NAI) is the leading non-profit, self-regulatory body focused on 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 over 100 member companies and continues to expand.

For nearly 20 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 digital advertising and related practices. These standards are set forth in the NAI Code of Conduct (referred to as the Code) which was initially adopted in 2000 with the unanimous support and praise of the U.S. Federal Trade Commission (FTC).

As advertising technology expanded to mobile devices, in 2013 the NAI published its first Mobile Application Code (App Code) to extend NAI standards to the mobile advertising ecosystem. The App Code was drafted to mirror the principles set forth in the Code while adding guidance specific to data collection and use through mobile applications. First updated in 2015, the App Code is now integrated into this 2018 Code of Conduct and ceases to exist as a separate document.

The Code imposes notice, choice, accountability, data security, and use limitation requirements on NAI member companies. NAI members are held to their promise to adhere to the Code through a rigorous compliance and enforcement program that includes annual reviews, ongoing technical monitoring, investigation of complaints, and enforcement procedures.

The Code is periodically reviewed and updated to anticipate and respond to rapidly evolving technologies and business models, as well as new issues raised by regulators and policymakers. Consequently, the Code was revised in 2008 and 2013, and updated in 2015. This 2018 update integrates the App Code, formerly a separate document, as well as recently-issued NAI Guidance.

Purpose of the 2018 Code

The 2018 Code of Conduct incorporates the requirements and guidance for NAI members previously found in the separate App Code. This integration allows NAI members, regulators, and the public to view NAI guidance for web and app-based data collection and use in a single document while streamlining compliance requirements.

The 2018 Code clarifies some existing terminology, including Non-Personally Identifiable Information (Non-PII), which is now referred to as Device-Identifiable Information (DII) to reduce potential confusion. The 2018 Code continues to recognize Interest-Based Advertising (IBA), Cross-App Advertising (CAA), and Retargeting as distinct practices, but refers to them collectively as "Personalized Advertising" to streamline requirements.

Scope of the Code

The Code governs only NAI member companies. It does not govern all data collection and use by member companies, but rather it is limited to members' Personalized Advertising and "Ad Delivery and Reporting" activities as defined herein.

The Code applies to members' Personalized Advertising and Ad Delivery and Reporting activities that: (1) occur in the United States or (2) apply to U.S. users. The NAI continues to monitor legislative and regulatory developments outside the U.S. and it encourages its members to apply the high standards of the Code on a global level, as many member companies do. At this time, however, only U.S.-based online advertising activities are subject to the NAI compliance program.

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 in the U.S. 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 only on behalf of a single first party. For example, collection and use of data on a single domain or mobile application, or a set of affiliated domains or applications, are not covered by the Code.

Consistent with the FTC's definition of "online behavioral advertising" and the DAA Principles, the Code does not govern "contextual advertising." Contextual advertising is the selection of an ad solely upon the content of the website or application on which it is served.

Member companies may use various technologies to engage in Personalized Advertising as business models cover traditional desktop web browsing, app usage on mobile devices and tablets, as well as the linking of such devices based on the assumption that they belong to the same user. The Code is intended to be technology-neutral, imposing obligations on members' Personalized Advertising activities regardless of the technologies used. The NAI continues to believe that all technologies, when used by members for Personalized Advertising, should provide users with an appropriate degree of transparency and control consistent with Code requirements. Due to the rapid pace of technological innovation in the digital advertising ecosystem, the NAI may publish from time to time additional guidance documents related to requirements in the Code.

The Code includes both code provisions and commentary. The purpose of the commentary sections in this Code is not to add substantive obligations on members or to alter the principles set forth in the Code itself. Instead, the commentary explains the intent behind certain provisions of the Code and provides non-binding illustrative guidance on methods through which members can meet the substantive obligations herein.

Relationship to the DAA's Principles and Guidance

In 2010, the NAI joined the Digital Advertising Alliance (DAA). Because the NAI Code applies only to NAI member companies, the DAA was founded to govern the entire digital ecosystem and impose obligations on website and application publishers as well as brand advertisers. The DAA is composed of six trade associations representing website and application publishers, internet service providers, cell phone carriers, social networks, advertisers, and offline data providers, *in addition* to the digital technology companies represented by the NAI. The DAA has developed Principles¹ governing data collection and use across unaffiliated websites and applications, and enforces those Principles through the Better Business Bureau (BBB) and the Direct Marketing Association (DMA).

The Code largely harmonizes with the DAA Principles as they apply to covered activities by NAI member companies. Thus, for example, the Code imposes an "enhanced" notice requirement for ads informed by Personalized Advertising. 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 Principles generally mirror the NAI's requirement for opt-out choice under the Code.

Unlike the DAA Principles, the NAI Code applies only to NAI members, and only to the extent those members are engaged in activities addressed by the Code.² Thus, obligations contained in the DAA Principles that are not applicable to third-party advertising companies are not included in the NAI Code. In some cases, obligations imposed on third-party advertising companies may be phrased differently in the Code than in the DAA Principles.

Because of the narrower scope of the NAI Code and its application only to member companies, this Code imposes obligations on NAI member companies beyond those currently required by the DAA Principles. These NAI-specific obligations include:

- 1) Completion of an annual review of the members' compliance with the NAI Code by NAI compliance staff;
- 2) Notice requirements for the prospective merger of Personally-Identifiable Information (PII) with Device-Identifiable Information (DII) to be used for Personalized Advertising purposes;
- 3) Disclosures regarding the collection and use practices of Ad Delivery and Reporting data;
- 4) Transparency with respect to all standard health-related interest segments used for Personalized Advertising;

¹ 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>; Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment (DAA Mobile Guidance), available at http://www.aboutads.info/DAA_Mobile_Guidance.pdf, (together DAA Principles).

² The NAI Code promotes actions by NAI members to increase trust in the entire Internet advertising ecosystem. For instance, members have an obligation to place use restrictions on data transferred to other parties. Members also take steps to require those websites and applications with which they have a contract and engage in Personalized Advertising to post notice regarding data collection and use practices for this purpose. However, the Code does not impose direct obligations on non-member companies and the NAI compliance program does not review the practices of non-members.

- 5) Opt-In Consent requirements for the use of “sensitive” health segments for Personalized Advertising;
- 6) Opt-In Consent requirements for the use of “sexual orientation” segments for Personalized Advertising;
- 7) Contractual notice requirements;
- 8) Data retention limits and disclosure obligations;
- 9) Reliable sources requirements;
- 10) Limitations on the transfer of data collected for Personalized Advertising; and
- 11) Access requirements for PII and associated DII used for Personalized Advertising.

Thus, the Code complements and enhances the DAA Principles. These additional obligations inform users and businesses that NAI member companies implement, honor, and maintain the NAI’s high standards for data collection for Personalized Advertising.

Framework of the Code

The fundamental principle underpinning the Code is that differing notice and choice obligations should apply depending on the sensitivity and proposed use of data. This basic principle, which has long been recognized by the NAI, is supported by the FTC’s Final Privacy Report³ and the White House Privacy Report,⁴ both issued in 2012. Both 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 should take into account the context in which the data is collected and used, principles that remain current today.

While arguments have been made⁵ that with adequate effort, all data points can ultimately be used to identify an individual, the NAI continues to find great value in providing an incentive for member companies to avoid collection and retention of directly identifiable data such as unencrypted name, email and postal address, telephone number, or social security number. As a result, most NAI member companies collect and retain only identifiers, such as cookie IDs and mobile advertising IDs, that are not intended to directly identify an individual.

³ FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (March 2012) (FTC Final Privacy Report), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>; see also Statement of Comm’r Maureen K. Olshausen, WC Docket No. 16-106, at 1-2 (FTC May 27, 2016), available at https://www.ftc.gov/system/files/documents/public_statements/951923/160527fccohlhausentmt1.pdf.

⁴ 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), <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>.

⁵ See, e.g., Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Arvind Narayanan & Ed Felten, *No Silver Bullet: De-Identification Still Doesn’t Work*, July 9, 2014, <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>.

To that end, this Code addresses 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) Personally-Identifiable Information (PII);
- 2) Device-Identifiable Information (DII); and
- 3) De-Identified Data.

PII refers to data that is used, or intended to be used, to directly identify a particular individual; DII refers to data that is linked, or intended to be linked, to a browser, device,⁶ or group of devices, but is not used, or intended to be used, to directly identify a particular individual; and De-Identified Data refers to data that is not linked to either an individual, browser, or device. In addition, the Code imposes obligations with respect to “Sensitive Data” and “Precise Location Data” use for Personalized Advertising. Sensitive Data includes specific types of PII that are sensitive in nature, as well as DII related to sensitive medical conditions and sexual orientation.

NAI Oversight and Monitoring

The NAI Code is a self-regulatory code. The NAI recognizes that the application of the Code may involve subjective judgements and that technical, operational, and policy questions may affect such judgements. For that reason, as a self-regulatory body, only 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 recommended steps to bring its practices into compliance, the NAI enforcement procedures allow the NAI to refer the matter to the FTC. In making such a referral, the NAI does not ask the FTC to interpret the Code, but simply to address the member’s failure to comply with the NAI’s interpretation and application of the Code.

⁶ At this time data collection and use through web browsers and applications are controlled by separate consumer choice mechanisms. “Device” refers to applications on smartphones or tablets that have access to device-wide controls and does not include data collection or use on websites accessed by browsers on that same device, which are subject to separate Opt-Out Mechanisms.

2018 NAI CODE OF CONDUCT

I. Definitions

A. AD DELIVERY AND REPORTING

Ad Delivery and Reporting is separate and distinct from Personalized Advertising, and means the collection or use of data about a browser 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, device, or time of day; statistical reporting, traffic analysis, analytics, or optimization 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, application, or device.

B. CROSS-APP ADVERTISING

Cross-App Advertising is the collection of data across applications owned or operated by different entities on a particular device for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected.

C. CROSS-DEVICE LINKING

Cross-Device Linking is the practice of linking two or more devices or browsers used or likely used by the same user, for advertising purposes.

D. DE-IDENTIFIED DATA

De-Identified Data is data that is not linked or intended to be linked to an individual, browser, or device.

E. DEVICE-IDENTIFIABLE INFORMATION (DII)

Formerly referred to as "Non-PII," Device-Identifiable Information (DII) is any data that is linked to a particular browser or device if that data is not used, or intended to be used, to identify a particular individual. DII may include, but is not limited to, unique identifiers associated with browsers or devices, such as cookie identifiers or advertising identifiers, and IP addresses, where such data is not linked or intended to be linked to PII. DII includes data that is linked to a series of browsers or devices linked through Cross-Device Linking, if that data is not used, or intended to be used, to identify a particular individual. DII does not include De-Identified Data.

F. INTEREST-BASED ADVERTISING

Interest-Based Advertising (IBA) is 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.

G. OPT-IN CONSENT

Opt-In Consent is an affirmative action taken by an individual that manifests the intent to opt in.

H. OPT-OUT MECHANISM

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

I. PERSONAL DIRECTORY DATA

Personal Directory Data is calendar, address book, phone/text log, or photo/video data (including any associated metadata), or similar data created by a user that is stored on or accessed through a device.

J. PERSONALIZED ADVERTISING

Personalized Advertising is a collective term for Interest-Based Advertising, Cross-App Advertising, and Retargeting, as well as any combination of these practices.

K. 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.

L. 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 radio frequency signal triangulation.

M. RETARGETING

Retargeting is the practice of collecting data about a browser's or device's activity in one unaffiliated web domain or application for the purpose of delivering an advertisement based on that data in a different, unaffiliated web domain or application.

N. 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.

II. Member Requirements

A. EDUCATION

1. Members shall collectively maintain an NAI website to serve as a centralized portal offering information about Personalized Advertising, the requirements of the NAI Code, information about, and/or centralized access to, user choice mechanisms.
2. Members should use reasonable efforts to inform individuals about Personalized Advertising and NAI-supported choices available to them with respect to Personalized Advertising.

B. TRANSPARENCY AND NOTICE

1. *Member Website Notice:* Each member company shall provide clear, meaningful, and prominent notice on its website that describes its data collection, transfer, and use practices for Personalized Advertising and Ad Delivery and Reporting. Such notice shall include:
 - a. A general description of the following, as applicable;
 - i. The Personalized Advertising and Ad Delivery and Reporting activities undertaken by the member company;
 - ii. The types of data collected or used for Personalized Advertising and Ad Delivery and Reporting purposes, including any PII, Precise Location Data, and Personal Directory Data;
 - iii. How such data will be used, including transfer, if any, to a third party;
 - iv. The technologies used by the member company for Personalized Advertising and Ad Delivery and Reporting, including any Cross-Device Linking for these purposes; and
 - v. The approximate length of time that data used for Personalized Advertising or Ad Delivery and Reporting will be retained by the member company;
 - b. A statement that the company is a member of the NAI and adheres to this Code;
 - c. A link to, or a description of how to access, an Opt-Out Mechanism for the company's Personalized Advertising across unaffiliated applications (if applicable); and
 - d. A link to an Opt-Out Mechanism for the company's Personalized Advertising across unaffiliated web domains (if applicable).
2. *Standard Health Segments:* Members that use standard interest segments for Personalized Advertising that are based on health-related information or interests shall disclose such segments on their websites.
3. *Publisher Website Notice:* Members shall take steps to require those websites with which they have a contract and engage in Personalized Advertising to clearly and conspicuously post notice containing, as applicable:
 - a. A statement of the fact that data may be collected for Personalized Advertising purposes on the website;

- b. A description of the types of data, including any PII, Precise Location Data, or Personal Directory Data, that are collected for Personalized Advertising purposes on the website;
 - c. An explanation of the purposes for which data is collected by, or will be transferred to, third parties, including Cross-Device Linking if applicable; and
 - d. A conspicuous link to an Opt-Out Mechanism for Interest-Based Advertising and Retargeting.
4. *Publisher App Store Notice:* Members shall take steps to require those applications with which they have a contract and engage in Personalized Advertising to clearly and conspicuously post notice, or a link to notice, in any store or on any website where the application may be acquired, when and where it is technically possible. Such notice shall contain, as applicable:
- a. A statement of the fact that data may be collected for Personalized Advertising purposes through the application;
 - b. A description of the types of data, including any PII, Precise Location Data, or Personal Directory Data, that are collected for Personalized Advertising purposes through the application;
 - c. An explanation of the purposes for which data is collected by, or will be transferred to, third parties, including Cross-Device Linking if applicable; and
 - d. A conspicuous link to, or a description of how to access, an Opt-Out Mechanism for Cross-App Advertising and Retargeting.
5. As part of members' overall efforts to promote transparency in the marketplace, members should make reasonable efforts to confirm that websites and applications where the member collects data for Personalized Advertising purposes furnish notices comparable to those described in II.B.3 and II.B.4 above, as applicable.
6. *Enhanced Notice:* Members shall provide, or support the provision or implementation of, notice of Personalized Advertising data collection and use practices and the NAI-supported choices available to users, in or around advertisements that are informed by such data, with the following exceptions:
- a. When notice is otherwise provided on the web page or application where the ad is served, outside of the publisher's privacy policy or terms of service;
 - b. When notice is provided in the application's settings and/or privacy policy and:
 - i. as part of the process of downloading an application to a device; or
 - ii. at the time the application is launched for the first time; or
 - iii. when the data is accessed.

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 DII for Personalized Advertising purposes shall require access to an Opt-Out Mechanism.
 - b. Use of PII to be merged with DII on a going-forward basis (prospective merger) for Personalized Advertising purposes 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 DII (retrospective merger) for Personalized Advertising purposes shall require a user's Opt-In Consent.
 - d. Use of Precise Location Data for Personalized Advertising shall require a user's Opt-In Consent or reasonable assurances that the application publisher has obtained Opt-In Consent on the member's behalf.
 - e. Use of Sensitive Data for Personalized Advertising purposes shall require a user's Opt-In Consent.
 - f. Use of Personal Directory Data for Personalized Advertising purposes shall require a user's Opt-In Consent.
2. An Opt-Out Mechanism for a member's web-based Personalized Advertising shall be made available on both the member's website and on the NAI website.
3. *User Control and Cross-Device Linking:* While a browser or device is opted out of Personalized Advertising by a member, that member shall:
 - a. Cease the collection of data for Personalized Advertising on the browser or device on which the user has expressed such choice, for use on that or any other browser or device associated through Cross-Device Linking; and
 - b. Cease Personalized Advertising on the browser or device on which the user has expressed such choice, with any data collected from a browser or device associated through Cross-Device Linking.
4. When a user has opted out of Personalized Advertising, 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 or device is opted out may not be used for Personalized Advertising regardless of the future opt-out status of the browser or device, and regardless of the technologies used by the member, absent Opt-In Consent.
5. The technologies that members use for Personalized Advertising purposes shall provide users with an appropriate degree of transparency and control.

D. USE LIMITATIONS

1. Members shall not create Personalized Advertising segments specifically targeting children under 13 without obtaining verifiable parental consent.
2. Members shall not use, or allow the use of, Personalized Advertising or Ad Delivery and Reporting data 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 making material changes to their policies and practices regarding Personalized 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 shall continue to be governed by the policy in effect at the time of its collection.

E. TRANSFER RESTRICTIONS

1. Members shall contractually require that any unaffiliated parties to which they provide PII for Personalized Advertising or Ad Delivery and Reporting purposes adhere to the provisions of this Code concerning PII.
2. Members shall contractually require that all parties to which they provide DII collected across web domains or applications owned or operated by different entities, not attempt to merge such DII with PII held by the receiving party or to otherwise re-identify the individual for Personalized Advertising purposes without obtaining the individual's Opt-In Consent. This requirement does not apply if the DII is proprietary data of the receiving party.

F. DATA ACCESS, QUALITY, SECURITY, AND RETENTION

1. Members retaining PII for Personalized Advertising purposes and not offering an Opt-Out Mechanism through which users can exercise their choice to exclude their PII and other information associated with PII, shall provide users with reasonable access to PII, and other information that is associated with PII, retained by the member for Personalized Advertising purposes.
2. Members shall conduct appropriate due diligence to help ensure that they obtain data used for Personalized 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 Personalized Advertising and Ad Delivery and Reporting purposes shall provide reasonable security for that data.
4. Members shall retain DII and PII collected for use in Personalized Advertising and Ad Delivery and Reporting 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 of Directors 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 and NAI designees, including in the course of annual compliance reviews and any investigation of a potential violation of the Code.
2. Some members may choose to subject policies and procedures related to Personalized Advertising or Ad Delivery and Reporting to review by NAI compliance staff or other NAI designees, even when those policies and procedures are not directly covered by the Code. In such instances attestations and public-facing privacy disclosures by the member will be included as part of the member's compliance review even if not directly covered by the Code, and failure to comply with such attestations and disclosures may be subject to NAI enforcement procedures.
3. 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.
4. 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 the complaints received.

C. USER COMPLAINTS

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

COMMENTARY TO THE 2018 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 CROSS-APP ADVERTISING

Interest-Based Advertising and Cross-App Advertising are defined as the collection of data across web domains or applications, respectively, owned or operated by different entities for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected.⁷ The FTC maintains the view that to treat domains or applications as owned or operated by the same entity, their corporate affiliation must be made clear to users by those entities.⁸ 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.” The same principle applies to data collection through applications, as covered by Cross-App Advertising.

Consistent with the FTC’s definition of “online behavioral advertising,” and DAA’s OBA Principles, the definitions of Interest-Based Advertising and Cross-App Advertising do not include “contextual advertising.”⁹ Contextual advertising means the ads are selected depending solely upon the content of the web page or application on which they are served. Contextual advertising also covers “first party” marketing, in which ads are customized or products are suggested based on the content of the site or application that the user is visiting at that time (including the content viewed, the searches performed, or the user’s location when viewing the page or application). Those activities are outside the scope of the Code.

RETARGETING

The Code defines Retargeting as the practice of collecting data about a user’s activity on a single web domain or application for the purpose of delivering an advertisement based on that data on a different, unaffiliated web domain or application. 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 or application, 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 and Cross-App Advertising because the advertisement may be selected based on activity on a single web domain or application and the user may not necessarily be included in an interest segment based on activity on multiple web domains or applications. Code requirements and obligations for Interest-Based Advertising or Cross-App Advertising apply equally to Retargeting.¹⁰

⁷ 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. The NAI will enforce the relevant NAI Code provisions on such members. The NAI will apply any future updates to the Code that cover provisioning of offline data for use in targeted advertising to all NAI members.

⁸ See FTC Final Privacy Report, *supra* note 3, at 42.

⁹ See FTC Final Privacy Report, *supra* note 3, at 41; DAA OBA Principles, *supra* note 1, at 10-11 (defining OBA to exclude first party activity, ad delivery and ad reporting, and contextual advertising).

¹⁰ 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 Formal Review of 23andMe, Inc., Case Number 30-2013 (2013) available at <http://www.bbb.org/us/storage/113/Documents/23andMe-Decision-20131115.pdf>.

PII, DII, AND DE-IDENTIFIED DATA

The Code divides data into three categories of “identifiability”: Personally-Identifiable Information (PII), Device-Identifiable Information (DII), 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 DII.
- 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.¹¹ The Report rejects a “bright line” test and instead adopts a scaled approach to evaluating risks and determining the obligations that attach to data. 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 DII,¹² the NAI believes that it is appropriate for the Code to continue to discourage members from linking the DII they collect with identified individuals for Personalized Advertising purposes. To encourage these data minimization efforts, the Code continues to distinguish between PII and DII and to impose different notice and choice requirements for each, with the level of protection required increasing with the “identifiability” and sensitivity of the data.¹³

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 Personalized 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 a 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 DII 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 or mobile advertising identifier, which would otherwise qualify as DII under the NAI Code, would be treated as PII if such an identifier is tied to PII, such as a name or email address.

¹¹ See FTC Final Privacy Report, *supra* note 3, 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).

¹² See *id.* at 18-19.

¹³ 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, the NAI may revise the labels, names, and definitions of different categories of data in future iterations of the Code.

DII

Formerly referred to in NAI Codes and Guidance as Non-PII, DII is defined as “data that is linked or reasonably linkable to a particular computer or device.” DII 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. DII does not include De-Identified Data.

Examples of how a member company may help ensure that the data it collects and uses for Personalized Advertising purposes meets this standard may be to: (1) take measures to help ensure that the data it collects or receives is not used to identify a particular individual, such as using only randomly generated numeric identifiers rather than names or email addresses; (2) publicly commit to maintain the data as DII; and/or (3) take reasonable steps, such as contractual measures, to prevent any companies with which it shares the DII from attempting to merge the data with PII or otherwise using the data to identify a particular individual (unless the DII is proprietary to the receiving party) for Personalized Advertising purposes.

De-Identified Data

The Code defines De-Identified Data as “data that is not linked or intended to be linked to an individual, browser, 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 DII, such as: (1) taking reasonable steps to ensure that the data cannot reasonably be connected or associated with an individual or with a particular browser 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 browser or device; and/or (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 browser 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.¹⁴

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, browser, or device which has then gone through a process that reasonably removes the links to any specific individual, browser, or device. For example, a member can remove or truncate identifiers (e.g., cookie identifiers, mobile advertising identifiers, and IP addresses) so that the data will reflect that a unique browser or device visited certain websites or applications, but the data will no longer be associated with a particular browser or device.

¹⁴ See DAA Multi-Site Data Principles, *supra* note 1, at 8.

PRECISE LOCATION DATA

The definition of “Precise Location Data” is meant to recognize that a range of technologies may be able to provide members the actual physical location of an individual with “reasonable specificity.” Please consult the NAI’s “Guidance for NAI Members: Determining Whether Location is Imprecise” for an in-depth analysis of how members may determine the precision of geolocation information.¹⁵

Accordingly, the definition of 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.¹⁶

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 Personalized 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 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 before using the data for Personalized 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 Personalized 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. Precise Location Data does not include information that does not necessarily reflect the actual location of a device such as the user’s speed and direction of travel, or a user-submitted check-in.

SENSITIVE DATA

Health

The definition of “Sensitive Data” includes two categories of health-related data: (1) data about a health condition or treatment derived from a sensitive source, and (2) data about certain sensitive conditions regardless of the source of the data. The collection and use of Sensitive Data for Personalized 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 Personalized Advertising that triggers the requirement for Opt-In Consent, regardless of which health or medical condition the segment references.

Second, Personalized 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

¹⁵ See Guidance for NAI Members: Determining Whether Location is Imprecise, available at https://www.networkadvertising.org/sites/default/files/nai_impreciselocation.pdf.

¹⁶ These examples are provided in this Code for illustrative purposes only.

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.”¹⁷ 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 conditions such as acne, allergies, dental, vision, heartburn, cold and flu, sinus, headache, back pain, first aid, sore throat, and cholesterol or blood sugar 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 Personalized 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 enforcement 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 Personalized Advertising that are related to health conditions or treatments (see the discussion of Health Transparency requirement, *infra* p. 18).

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 Personalized Advertising without obtaining Opt-In Consent. The Code does *not* intend to prohibit Retargeting based on visits to generalized 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 specifically 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 Personalized Advertising.

¹⁷ 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 or applications associated with particular conditions or treatments so that advertisers can serve contextual advertising on those sites or applications.

II. Member Requirements

MEMBER-PROVIDED NOTICE (§ II.B.1)

Section II.B.1 of the NAI Code requires members to provide clear, meaningful, and prominent notice concerning their data collection practices. This requirement is not limited to Personalized 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 or instructions for opting out on mobile devices. 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 Personalized Advertising purposes.

Members should 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 Personalized Advertising and Ad Delivery and Reporting, including Cross-Device Linking. Member companies are *not* required to disclose the technologies they use with a level of specificity that would reveal their proprietary business models.

The 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. The 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 Personalized 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 Personalized Advertising.

NAI member companies using health-related interest segments created exclusively with Opt-In Consent from users are not obligated to disclose such segments under the Health Transparency requirement, as the segments are disclosed to users at the time consent is obtained.

WEBSITE AND APP STORE NOTICE (§ II.B.3-6)

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

If an NAI member company has a direct contractual relationship with a website or application where it conducts Personalized Advertising, it shall take steps to contractually require the website or application to post notice of Personalized Advertising and a link to or instructions for accessing an Opt-Out Mechanism.¹⁸ The steps may comprise of 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, app store, or separate footer link, such as “About Our Ads.” In a mobile application environment, this provision of the Code is intended to help ensure, to the extent practicable, that users are provided notice of Personalized Advertising prior to acquiring an application, recognizing that members are generally unable to provide such notice themselves, because they do not control the application or the app store.

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. For example, members may regularly check a reasonably-sized sample of the websites and applications where they conduct Personalized Advertising to ensure that the websites and applications provide appropriate notice, following up with those that do not.¹⁹

Enhanced Notice Requirement (§ II.B.6)

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 Personalized 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 Personalized 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 Personalized Advertising without enhanced notice, the NAI member should decline to conduct the campaign. Finally, the NAI will continue to work with DAA and DAA member organizations to educate advertisers and publishers on the requirements of the DAA program.

¹⁸ The requirement to contractually require a website or application 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 Personalized 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 Personalized Advertising purposes.

¹⁹ 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 Personalized Advertising purposes only where they serve ads. Member companies that provide in-ad notice pursuant to Section II.B.6 and only collect data for Personalized 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.

USER CONTROL (§ II.C)

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

The Code requires members to provide an Opt-Out Mechanism for users wishing to exercise choice regarding the collection and use of DII for Personalized Advertising purposes. The Code also requires that members obtain Opt-In Consent for the collection and use of Sensitive Data, Precise Location Data, and Personal Directory Data for Personalized Advertising. Members must also obtain Opt-In Consent for the retrospective merger²⁰ of PII and DII for Personalized Advertising purposes. For the prospective merger of PII and DII for Personalized 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 DII to be merged with PII and how the merged data would be used for Personalized Advertising purposes.

Choices regarding Cross-Device Linking (§ II.C.3)

In 2017 the NAI published, and began enforcement of, its Guidance regarding Cross-Device Linking.²¹ This document clarifies that Code requirements apply to Cross-Device Linking and instructs members how to provide notice and choice for such technology. While a browser or device is opted out from Personalized Advertising by a member company, the member shall effectively remove that browser or device from a device “map” for Personalized Advertising purposes and shall cease collecting data on the browser or device for Personalized Advertising use on any associated browser or device. Similarly, the member shall cease Personalized Advertising on the opted-out browser or device with data from any associated browser or device. These requirements are in addition to any other Code requirements regarding Personalized Advertising or Ad Delivery and Reporting on a given browser or device. Members may continue to engage in Cross-Device Linking for Ad Delivery and Reporting purposes, such as attribution.

Honoring Opt-Out Choices (§ II.C.4)

Following an opt-out, member companies must cease collecting and using data for Personalized Advertising purposes for that browser or device.²² Member companies may, however, continue to collect data for other purposes, such as Ad Delivery and Reporting. Any data collected while a browser or device is opted out may not be used for Personalized Advertising purposes, regardless of the future opt-out status of the browser or device, or the technology used for Personalized Advertising. For example, a user opts out of Personalized 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 Personalized Advertising, even after the opt-out choice is deleted. Of course, a user may always choose to have such data used for Personalized Advertising by providing the member company with express, affirmative consent.

²⁰ For the purpose of this Code, “retrospective merger” is the combination of PII with previously collected DII by a member. This could include the merger of existing segment information with a newly collected name or email address. When the individual’s DII was originally collected, the individual did not have the expectation that it would later be tied to his or her PII. “Prospective merger” is the combination of PII with DII to be collected on a going-forward basis by a member. The PII was collected by the member before the DII 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.

²¹ See Guidance for NAI Members: Cross-Device Linking, available at https://www.networkadvertising.org/pdfs/NAI_Cross_Device_Guidance.pdf.

²² The NAI recognizes that separate Opt-Out Mechanisms control each browser on a device, as well as a mobile device’s app environment, *supra* note 6.

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

While members may continue to collect and use data for purposes other than Personalized 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 membership application and annual review processes to ensure that its Opt-Out Mechanism, at a minimum, results in the cessation of Personalized Advertising for the applicable browser or device. While the NAI is working to expand the scope of its Code, some responsible actors, with business models that are related to Personalized 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 Mechanism to be consistent with the representations made to NAI staff and will hold members accountable for their representations through the NAI's enforcement procedures even if the opt-out may otherwise comply with NAI Code requirements.

Technologies Used for Personalized Advertising (§ II.C.5)

The NAI recognizes that new business models are in development and that technologies are evolving rapidly. As part of that process, the 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.²³ The NAI intends to remain technology-neutral while helping to ensure the overall health of the digital advertising ecosystem. In order to address the use of new technologies in a web environment the NAI published its Guidance on the use of Non-Cookie Technologies for Interest-Based Advertising, which it began enforcing in 2017.²⁴

As NAI members develop new business models utilizing non-cookie technology, the NAI urges that they seek to implement these business models with the principles of the NAI Code in mind. The NAI strives to provide a means through which its members may provide a robust and lasting Opt-Out Mechanism but recognizes that such an endeavor can be challenging due to evolving cookie controls instituted by some browser manufacturers, which can make it difficult for a persistent opt-out to be placed on a browser. The 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.

²³ See FED. TRADE COMM'N, *PRIVACY ONLINE: A REPORT TO CONGRESS 7* (1998), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>; see also FED. TRADE COMM'N, *PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE* (2000), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

²⁴ See Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising, available at https://www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf.

USE LIMITATIONS (§ II.D)

Children (§ II.D.1)

The Code prohibits member companies from creating segments for Personalized 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 Personalized 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.²⁵ Users are made aware, through in-ad notice and privacy policies of website and application 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 Personalized Advertising purposes or the merger of DII with PII when a member previously represented that it does not engage in these activities. Changes are not considered "material" for the purposes of this provision if they result in reduced collection or use of data, or when a company changes its disclosures to provide greater transparency about its existing practices. The 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 for Personalized Advertising purposes to unaffiliated third parties. These are extensions of the requirements set forth above for data to be treated as DII rather than PII under the Code. For instance, under the Code, members maintain the DII status of data by contractually requiring that all parties to whom they provide DII collected across web domains or applications owned or operated by different entities not attempt, for Personalized Advertising purposes, to merge such DII with PII held by the receiving party without obtaining the individual's Opt-In Consent (unless the DII 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)

To foster transparency and control where PII is associated with DII, the Code requires member companies to provide reasonable access to any PII and associated DII collected and used for Personalized Advertising purposes or to provide users with a method of opting out their PII and any associated data from Personalized Advertising uses. However, the Code does *not* require companies to provide access to DII that is *not* associated with PII.

²⁵ See White House Privacy Report, *supra* note 3, 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 with access to DII-based interest segments associated with their browsers or devices. 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 DII 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 self-regulatory 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 data storage and architecture may vary from member to member, member companies, not NAI staff, are in the better position to determine which security measures are appropriate under a given set of circumstances.

DATA RETENTION (§ II.F.4)

The NAI Code requires member companies to keep DII (or any PII used for Personalized 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.a.v, member companies are required to publicly disclose the period of time for which they retain such data for those purposes. At the end of that publicly-stated retention period, members are required to either delete or de-identify such 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