



2020

NAI Code of Conduct

INTRODUCTION

The Network Advertising Initiative (NAI) is the leading non-profit, self-regulatory body focused on advertising technology providers in the online advertising ecosystem. Created during the nascence of the online advertising industry in 2000, the NAI is one of the Internet's longest standing and most respected industry self-regulation efforts. The NAI currently has over 100 member companies and continues to expand.

For nearly twenty years the NAI has developed and enforced self-regulatory standards that establish sound data management practices with respect to the collection and use of data for Tailored Advertising and related practices. These self-regulatory standards are set forth in this 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 was integrated into the 2018 Code of Conduct and ceased to exist as a separate document. The NAI has also published more detailed information for members engaging in specific ad-related activities in Guidance for NAI Members on the topics of Cross-Device Linking, Viewed Content Advertising, Use of Non-Cookie Technologies for Interest-Based Advertising, and Determining Whether Location Is Imprecise.

The Code imposes notice, choice, accountability, data security, and use limitation requirements on NAI member companies. The NAI holds its members to their promise to adhere to the Code and Guidance through a rigorous compliance and enforcement program that includes annual reviews, investigation of complaints, and enforcement procedures when appropriate. Additionally, the NAI's compliance initiatives include the use of technological monitoring tools that aim to identify possible problems or violations at an early stage, so that member companies may promptly address them.

The NAI and its Board of Directors periodically review and update the Code to anticipate and respond to rapidly evolving technologies and business models, as well as new issues raised by regulators and policymakers. For example, the Code was revised in 2008 and 2013, and updated in 2015 and 2018. This 2020 revision modernizes certain terminology and codifies many members' existing practice of applying NAI principles to the use of data originating offline for digital advertising, making this now a general member requirement. The expanded definition of Tailored Advertising, now including Audience-Matched Advertising, covers the use of such data to target advertising across sites, applications, and on covered devices.

Purpose of the 2020 Code

Notwithstanding modest updates in 2015 and 2018, the last significant revision to the Code took place in 2013. Since then the market has witnessed a rapid maturation of the mobile advertising ecosystem, expanding use of offline data for online ad targeting, the proliferation of linking devices for targeted advertising (including on televisions), and an evolution in the dialogue regarding data identifiability due to technological advances. These issues are addressed in the revised Code. The 2020 Code incorporates the Guidance for NAI Members: Viewed Content Advertising, which expanded the scope of the NAI's self-regulatory efforts to data collection and use on televisions for Tailored Advertising upon its release in 2018. The 2020 Code also adds several new definitions, and revisits a few existing ones including the concept of data identifiability in the form of Device-Identified Information (DII) and Personally-Identified Information (PII).

The scope of the Code officially expands to cover an area in which it has been applied by a majority of member companies for a number of years: the use of user-level offline data for targeted advertising across websites and applications, as well as on covered devices. This change effectively codifies the current practices of most NAI members and will now be enforced as a Code requirement to ensure uniformity in the treatment of such data across the NAI's entire membership. Finally, this Code also establishes certain transparency requirements for members' use of data to engage in Tailored Advertising on behalf of political campaigns, and expands Opt-In Consent requirements for additional uses of Sensitive Information, Precise Location Information, Sensor Information, and Personal Directory Information.

Scope of the Code

The Code governs only NAI member companies. It does not govern all data collection by member companies, but rather it is limited to members' Tailored Advertising and Ad Delivery and Reporting activities as defined herein. To the extent a member company collects or uses previously collected data about a user, browser, or device for the purpose of either delivering advertisements or providing advertising-related services on unaffiliated websites and applications as well as on covered devices, that activity is governed by the Code.

The Code applies to members' Tailored 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.

Consistent with the FTC's definition of "online behavioral advertising" and the DAA Principles¹, the Code does not govern "contextual advertising," which is based solely on the context of a website, application, or viewed content.

Member companies may use various technologies to engage in Tailored Advertising as business models cover traditional desktop web browsing in addition to activity on mobile devices, tablets, and on covered devices, 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' Tailored Advertising activities regardless of the technologies used. The NAI continues to believe that all technologies, when used by members for Tailored Advertising, should provide users with an appropriate degree of transparency and control consistent with Code requirements. Due to the rapid pace of innovation in the digital advertising ecosystem, the NAI may publish from time to time additional guidance documents related to Code requirements.

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).

The Code includes both code provisions and explanatory 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, along with five other trade associations, helped form the Digital Advertising Alliance (DAA). The DAA has developed Principles governing data collection and use across unaffiliated websites and applications, and enforces these through the Better Business Bureau (BBB) and the Data and Marketing Association (DMA). The DAA is composed of trade associations representing website and application publishers, internet service providers, cell phone carriers, social networks, advertisers, offline data providers, as well as the digital technology companies represented by the NAI. Consequently, the DAA Principles govern the entire digital advertising ecosystem and impose obligations not only on advertising technology companies but also on website publishers and brand advertisers.

Because the DAA Principles apply to the entire digital advertising ecosystem, they are by nature broader and in some cases less restrictive than the NAI Code, which only applies to member companies that agree to adhere to NAI requirements. However, 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 Tailored 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.

Unlike the DAA Principles, the NAI Code applies only to NAI members, and only to the extent they 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, in some instances this Code imposes obligations on NAI member companies beyond those required by the current DAA Principles. NAI-specific obligations intended to establish a strong Code compliance framework for members include:

- 1) Completion of an annual review of the members’ compliance with the NAI Code and Guidance by NAI compliance staff;³
- 2) Robust Notice and Opt-In Consent requirements for the use of Personally-Identified Information (PII), including merger with Device-Identified Information (DII), for Tailored Advertising purposes;

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 Tailored 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.

³ The annual review is bolstered by the use of the NAI’s proprietary compliance assessment tools used, for example, to confirm when a member has changed its privacy policy.

- 3) Disclosures regarding data collection and use practices for Ad Delivery and Reporting;
- 4) Transparency with respect to all standard “health-related” interest segments used for Tailored Advertising;
- 5) Transparency with respect to all standard “political” interest segments used for Tailored Advertising;
- 6) Opt-In Consent requirements for the use of “sensitive” health segments for Tailored Advertising and Ad Delivery and Reporting;
- 7) Opt-In Consent requirements for the use of “sexual orientation” segments for Tailored Advertising and Ad Delivery and Reporting;
- 8) Contractual requirements for partner-provided notice;
- 9) Data retention limits and disclosure obligations;
- 10) Requirements for vetting data sources;
- 11) Limitations on the transfer of data collected for Tailored Advertising;
- 12) Deletion requirements for PII and associated DII used for Tailored Advertising;
- 13) Notice and consent requirements related to Audience-Matched Advertising; and
- 14) Notice and consent requirements related to data collection and use on televisions and peripheral devices.

Thus, the Code incorporates and expands on the DAA Principles, and the NAI employs a robust, member-specific compliance review process in an effort to quickly gauge compliance. These additional obligations inform users and businesses that NAI member companies implement, honor, and maintain the NAI’s high standards for data collection and use for Tailored 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 2012 Final Privacy Report and the 2012 White House Privacy Report.⁴ 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 take into account the context in which the data is collected and used.

⁴ FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (March 2012) (FTC Final Privacy Report), available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/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 <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>.

While arguments have been made that with adequate effort⁵ a variety of data points can ultimately be used to identify an individual, the NAI continues to find great value in providing an incentive for member companies, where possible, to avoid collection and retention of directly identifying data such as plaintext name, email and postal address, telephone number, or social security number. As a result, many NAI member companies collect and retain only those identifiers that are not intended to directly identify an individual, such as cookie identifiers, mobile advertising identifiers, and in some instances, hashed email addresses.

Recognizing the evolving discussion around identifiability, however, this Code adopts updated terminology and definitions to maintain the focus on how member companies treat and maintain data in relation to the identifiers to which that data is tied, rather than on the hypothetical identifiability of data in a manner divorced from real-world privacy consequences to users.

To that end, this Code classifies identifiers into three categories and imposes different obligations on NAI members based on the sensitivity and use of the data. These three categories are:

- 1) Personally-Identified Information (PII);
- 2) Device-Identified Information (DII); and
- 3) De-Identified Information.

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

The NAI Code was originally drafted to address data collection and use for targeted advertising on web browsers, referred to as Interest-Based Advertising. As technology evolved, the NAI expanded the scope of its Code to also cover data collection and use for digital advertising in mobile applications, known as Cross-App Advertising, and most recently to data collection and use on televisions, through Viewed Content Advertising. Increasingly, these activities are combined through reliance on Cross-Device Linking to provide relevant advertising across devices. Because the web, application, and television environments differ in the methods through which NAI members are able to provide users with notice and choice, the NAI continues to define Interest-Based Advertising, Cross-App Advertising, and Viewed Content Advertising as separate activities. However, these three activities, along with Retargeting and Audience-Matched Advertising, are considered Tailored Advertising. This enables the NAI to maintain its high standards for ensuring user privacy across all environments while adapting certain requirements to better suit the notice and choice possibilities on specific types of devices. Because of the expanded scope of this Code, in addition to mobile phones and tablets, use of the term “device” now also includes televisions and peripheral devices such as digital media players and gaming consoles.

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

Platforms and Technology Providers

Some NAI members do not themselves engage in Tailored Advertising, but provide technologies or platforms that enable others to engage in such activities. These members may not always have visibility into the way their partners or clients may use their technology or platform. The NAI is mindful of the limitations this may place on such members' ability to monitor compliance with the Code, but expects such members to pass any relevant Code requirements and restrictions to their clients and partners through contractual means. As an example, if members are unable to verify whether their technology or platform is used by others to collect Sensitive Information for Tailored Advertising, these members are expected to contractually prohibit such activity without a user's Opt-In Consent.

NAI Oversight and Monitoring

The NAI Code is a self-regulatory code. The NAI recognizes that the application of the Code and Guidance may involve subjective judgments and that technical, operational, and policy questions may affect such judgments. For that reason, as a self-regulatory body, the NAI is the final arbiter of how the Code and Guidance apply to its members' practices in any given instance. Only NAI staff is authorized to interpret the requirements of the Code and Guidance and to evaluate compliance with and enforce violations of the Code or Guidance. If NAI staff determines that there is an instance of non-compliance with the Code or Guidance 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 or Guidance, but simply to address the member's failure to comply with the NAI's interpretation and application of the Code or Guidance.

2020 NAI CODE OF CONDUCT

I. Definitions

A. AD DELIVERY AND REPORTING (ADR)

Ad Delivery and Reporting (ADR) is separate and distinct from Tailored Advertising, and it refers to 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, time of day, or real-time precise location; statistical reporting, traffic analysis, analytics, optimization of ad placement; ad performance, reach, and frequency metrics (including frequency capping); sequencing of advertising creatives; billing; and logging the number and type of ads served on a particular day to a particular website, application, or device. ADR does not include data collection and use for security and fraud prevention. If data collected through ADR is later used to tailor advertising based on interests known or inferred from such data, such use shall be treated as Tailored Advertising under this Code.

B. AUDIENCE-MATCHED ADVERTISING (AMA)

Audience-Matched Advertising (AMA) is the practice of using data linked, or previously linked, to Personally-Identified Information (PII) for the purpose of tailoring advertising on one or more unaffiliated web domains or applications, or on devices, based on preferences or interests known or inferred from such data.

C. CROSS-APP ADVERTISING (CAA)

Cross-App Advertising (CAA) is the collection of data through applications owned or operated by different entities on a particular device, or the use of such data, for the purpose of tailoring advertising based on preferences or interests known or inferred from the data collected.

D. CROSS-DEVICE LINKING

Cross-Device Linking is the practice of linking two or more devices or browsers known or reasonably believed to belong to the same user or household, for Tailored Advertising or Ad Delivery and Reporting.

E. DE-IDENTIFIED INFORMATION

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

F. DEVICE-IDENTIFIED INFORMATION (DII)

Device-Identified 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 directly 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 to PII. DII includes data that is linked to a series of browsers or devices associated through Cross-Device Linking, if that data is not used to directly identify a particular individual. DII does not include De-Identified Information.

G. INTEREST-BASED ADVERTISING (IBA)

Interest-Based Advertising (IBA) is the collection of data across web domains owned or operated by different entities, or the use of such data, for the purpose of tailoring advertising based on preferences or interests known or inferred from the data collected.

H. OPT-IN CONSENT

Opt-In Consent is an affirmative action taken by a user that manifests the intent to opt in to an activity described in a clear and conspicuous notice. An NAI member may obtain Opt-In Consent directly from a user, or through reasonable assurances that a partner interacting directly with the user has obtained such consent on the member's behalf.

I. OPT-OUT MECHANISM

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

J. PERSONAL DIRECTORY INFORMATION

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

K. PERSONALLY-IDENTIFIED INFORMATION (PII)

Personally-Identified Information (PII) is any data linked, or intended to be linked, to an identified individual, including name, address, telephone number, email address, financial account number, and non-publicly available government-issued identifier.

L. PRECISE LOCATION INFORMATION

Precise Location Information is data 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, or the use of such data, for the purpose of customizing an advertisement in a different, unaffiliated web domain or application, or on a separate covered device.

N. ROBUST NOTICE

Robust Notice is the provision of clear and conspicuous notice, directly adjacent to a PII entry field or submit button, at the time and place of collection of PII for Tailored Advertising purposes.

O. SENSITIVE INFORMATION

Sensitive Information includes:

- Social Security Numbers or other non-publicly available 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, conditions predominantly affecting or associated with children and not treated with over-the-counter medication, mental health-related conditions, and sexually transmitted diseases (the condition or treatment is sensitive regardless of the source); and
- Information, including inferences, about a user's sexual orientation.

P. SENSOR INFORMATION

Sensor Information includes information from a camera, microphone, or any sensor on a user's device that may collect biometric data from such device. Sensor Information does not include information such as barometric pressure or accelerometer data that is used to determine the status of the device, alone or in combination with Precise Location Information.

Q. TAILORED ADVERTISING

Tailored Advertising is the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device. Tailored Advertising includes Interest-Based Advertising, Cross-App Advertising, Audience-Matched Advertising, Viewed Content Advertising, and Retargeting. Tailored Advertising does not include Ad Delivery and Reporting, including frequency capping or sequencing of advertising creatives.

R. VIEWED CONTENT ADVERTISING

Viewed Content Advertising is the collection of Viewed Content Information, or the use of such data for the purpose of tailoring advertising based on preferences or interests known or inferred from the data collected.

S. VIEWED CONTENT INFORMATION

Viewed Content Information is data about the video content viewed on a television.

II. Member Requirements

A. EDUCATION

1. Members shall collectively maintain an NAI website to serve as a centralized portal offering education about Tailored Advertising, the requirements of the NAI Code, and information about, and/or centralized access to, user choice mechanisms.
2. Members shall use reasonable efforts to educate users about Tailored Advertising and the choices available to them with respect to Tailored 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 Tailored Advertising and Ad Delivery and Reporting. Such notice shall include:
 - a. A general description of the following, as applicable;
 - i. The Tailored Advertising and Ad Delivery and Reporting activities undertaken by the member company;
 - ii. The types of data collected or used for Tailored Advertising and Ad Delivery and Reporting purposes, including any PII, Sensitive Information, Viewed Content Information, Precise Location Information, Sensor Information, and Personal Directory Information (if applicable);
 - iii. How such data will be used, including transfer, if any, to third parties;
 - iv. The technologies used by the member company for Tailored Advertising and Ad Delivery and Reporting, including any non-cookie technologies and Cross-Device Linking for these purposes; and
 - v. The approximate length of time that DII and PII used for Tailored Advertising and/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 Tailored Advertising across unaffiliated applications (if applicable);
 - d. A link to, or a description of how to access, an Opt-Out Mechanism for the company's Tailored Advertising on a television (if applicable);
 - e. A link to an Opt-Out Mechanism for the company's Tailored Advertising across unaffiliated web domains (if applicable); and
 - f. A link to an Opt-Out Mechanism linked to PII for the company's use of PII or hashed PII for Tailored Advertising (if applicable).

2. *Health Segments:* Members that use interest segments for Tailored Advertising that are based on health-related information or interests shall disclose such segments on their websites. Members using standard interest segments shall disclose a list of all such segments. Members using custom interest segments shall disclose a representative sample of such segments.
3. *Political Segments:* Members that use interest segments for Tailored Advertising that are based on political information or interests shall disclose such segments on their websites. Members using standard political interest segments shall disclose a list of all such segments. Members using custom political interest segments shall disclose a representative sample of such segments.
4. *Publisher Website Notice:* Members shall take steps to require those websites with which they have a contract and engage in Tailored Advertising to clearly and conspicuously post notice which contains, as applicable:
 - a. A statement of the fact that data may be collected or used for Tailored Advertising purposes on the website;
 - b. A description of the types of data, including any PII, Sensitive Information, Precise Location Information, Sensor Information, or Personal Directory Information, that are collected for Tailored 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 and Audience-Matched Advertising if applicable; and
 - d. A conspicuous link to an Opt-Out Mechanism for web-based Tailored Advertising.
5. *Publisher App Store Notice:* Members shall take steps to require those applications with which they have a contract and engage in Tailored 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 or used for Tailored Advertising purposes through the application;
 - b. A description of the types of data, including any PII, Sensitive Information, Viewed Content Information, Precise Location Information, Sensor Information, or Personal Directory Information, that are collected for Tailored 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 and Audience-Matched Advertising if applicable; and
 - d. A conspicuous link to, or a description of how to access, an Opt-Out Mechanism for application-based Tailored Advertising.

6. *Viewed Content Advertising Partner Notice:* Members shall take steps to require those partners with which they have a contract and engage in Viewed Content Advertising to clearly and conspicuously post notice, or a link to notice, on the screen or most appropriate user interface, when technically possible, as applicable. Such notice shall contain, as applicable:
 - a. A statement of the fact that data may be collected or used for Viewed Content Advertising purposes through the television;
 - b. A description of the types of data, including any PII, Sensitive Information, Viewed Content Information, Precise Location Information, Sensor Information, or Personal Directory Information, that are collected for Tailored Advertising purposes through the television;
 - c. An explanation of the purposes for which data is collected by, or will be transferred to, third parties, including Cross-Device Linking and Audience-Matched Advertising, if applicable; and
 - d. A conspicuous link to, or a description of how to access, an Opt-Out Mechanism for Viewed Content Advertising on the screen or most appropriate user interface.
7. As part of members' overall efforts to promote transparency in the marketplace, members should make reasonable efforts to confirm that websites, applications, and Viewed Content Advertising partners from which the member directly or indirectly collects data for Tailored Advertising purposes furnish notices comparable to those described in sections II.B.4–II.B.6 above, as applicable. When not contracting directly with publishers, members should only contract with intermediaries who have similar requirements for the publishers or other downstream parties they represent.
8. *Enhanced Notice:* Members shall provide, or support the provision or implementation of, notice of Tailored 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 or device'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 during a device's initial setup process; or
 - iii. When the data is first 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 Tailored Advertising purposes shall require access to an Opt-Out Mechanism.
 - b. Use of hashed PII for Audience-Matched Advertising shall require access to an Opt-Out Mechanism linked to PII.
 - c. Use of PII alone, or to be merged with DII collected on a going-forward basis, for Tailored Advertising shall require Robust Notice at the time of PII collection as well as access to an Opt-Out Mechanism linked to PII.
 - d. Use of PII to be merged with previously collected DII for Tailored Advertising shall require Robust Notice at the time of PII collection, a user's Opt-In Consent, and access to an Opt-Out Mechanism linked to PII.
 - e. Use of Sensitive Information for Tailored Advertising or Ad Delivery and Reporting purposes shall require a user's Opt-In Consent.
 - f. Use of Precise Location Information for Tailored Advertising or Ad Delivery and Reporting purposes shall require a user's Opt-In Consent.
 - g. Use of Personal Directory Information for Tailored Advertising or Ad Delivery and Reporting purposes shall require a user's Opt-In Consent.
 - h. Use of Sensor Information for Tailored Advertising or Ad Delivery and Reporting purposes shall require a user's Opt-In Consent.
 - i. Collection of all or substantially all Viewed Content Information from a television for Viewed Content Advertising shall require a user's Opt-In Consent.
2. An Opt-Out Mechanism for a member's web-based Tailored Advertising shall be made available on both the member's website and on the NAI website.
3. An Opt-Out Mechanism for a member's use of PII or hashed PII shall apply to the member's use of that PII or hashed PII for Tailored Advertising on all devices and shall be made available on both the member's website and on the NAI website. If an NAI member uses types of PII or hashed PII that are not supported by the NAI Opt-Out Mechanism, and are not linked to the types of PII or hashed PII supported by the NAI Opt-Out Mechanism, the member shall provide an Opt-Out Mechanism for such PII or hashed PII directly on the member's site.

4. *User Control and Cross-Device Linking*: While a user is opted out of Tailored Advertising by a member, that member shall:
 - a. Cease the collection of data for Tailored Advertising on the browser or device for which the user has expressed their choice, for use on that or any other browser or device associated through Cross-Device Linking; and
 - b. Cease Tailored Advertising on the browser or device for which the user has expressed their choice, with any data collected from a browser or device associated through Cross-Device Linking.
5. When a user has opted out of Tailored Advertising, member companies may continue to collect data for other purposes, including Ad Delivery and Reporting, unless noted otherwise in the Code. However, any data collected by a member company from a browser or device while that browser or device is opted out may not be used for Tailored 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.
6. The technologies that members use for Tailored Advertising purposes shall provide users with an appropriate degree of transparency and control.

D. USE LIMITATIONS

1. Members shall not create Tailored Advertising segments specifically targeting children under 16 without obtaining verifiable parental consent.
2. Members shall not use, or allow the use of, data collected as a result of Tailored Advertising or Ad Delivery and Reporting for any non-marketing eligibility purposes, including:
 - a. Employment Eligibility;
 - b. Credit Eligibility;
 - c. Health Care Eligibility;
 - d. Insurance Eligibility and Underwriting and Pricing;
 - e. Tenancy Eligibility; and
 - f. Education Admissions.
3. Members making material changes to their policies and practices regarding Tailored 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 or make available PII for Tailored Advertising or Ad Delivery and Reporting purposes adhere to the provisions of this Code concerning PII, including notice, user control, access, downstream transfer restrictions, and uses for non-marketing eligibility purposes. This requirement does not apply if the PII is proprietary data of the receiving party.
2. Members shall contractually require that all parties to which they provide or make available DII, collected as part of the member's Tailored Advertising and Ad Delivery and Reporting activities, not attempt to merge such DII with PII held by the receiving party or to otherwise re-identify the individual for Tailored Advertising purposes. This requirement does not apply if the DII is proprietary data of the receiving party, or if the receiving party provides the user with Robust Notice at the time of data collection, and/or obtains the user's Opt-In Consent as detailed in sections II.C.1.c-d above.

F. DATA ACCESS, QUALITY, SECURITY, AND RETENTION

1. Members retaining PII for Tailored Advertising purposes shall provide users with:
 - a. Reasonable access to PII, and other information that is associated with PII, retained by the member for Tailored Advertising purposes; and
 - b. An Opt-Out Mechanism through which users can choose to exclude their PII from further Tailored Advertising, as required in section II.C.3 above, and additionally to request that the member permanently delete information that is associated with the user's PII except for the user's opt-out preference.
2. Members shall conduct appropriate due diligence to help ensure that they obtain data used for Tailored Advertising from responsible sources that provide users with appropriate levels of notice and choice. As part of this due diligence process, members shall require partners providing matching services for Audience-Matched Advertising to offer an Opt-Out Mechanism linked to PII as described in section II.C.1.b above.
3. Members that collect, transfer, or store data for use in Tailored Advertising and Ad Delivery and Reporting shall provide reasonable security measures to protect that data.
4. Members shall retain DII and PII collected for use in Tailored Advertising and Ad Delivery and Reporting only as long as necessary for the purpose for which the data was collected, to fulfill another 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 relevant business practices adhere to the Code, as supplemented by applicable implementation Guidance 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 that are related to Tailored 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 these policies shall also articulate the penalties that could be imposed for a finding of noncompliance, including referral of the matter to appropriate regulatory agencies, such as 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, 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 Tailored 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 2020 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 also provides examples of some possible measures member companies may take to meet the substantive obligations of the Code. Such examples are neither exclusive nor exhaustive.

Definitions

AUDIENCE-MATCHED ADVERTISING

Audience-Matched Advertising is the practice of using data linked, or previously linked, to Personally-Identified Information (PII) for the purpose of tailoring advertising on unaffiliated web domains or applications, or on devices, based on preferences or interests known or inferred from such data. This data may be collected in an offline setting, such as when a user signs up to receive a catalog, or provides an email address at a physical retail outlet. This data may also be collected online through a retailer’s website or application while a user is making a purchase, outside the context of Interest-Based Advertising or Cross-App Advertising. If such data is later used to tailor advertising on unaffiliated websites or applications, or on devices covered by the Code, it is Audience-Matched Advertising.

This practice typically does not involve the use of PII to target users. Rather, encrypted or hashed PII is matched between an advertiser’s customer record management (CRM) database and an online authentication point, or match partner, and only information or inferences regarding a user’s interests or demographic information is linked to DII such as a cookie ID or mobile advertising ID.

If PII is not hashed before its use for Tailored Advertising, or if an NAI member intends to re-identify users after engaging in Audience-Matched Advertising, the NAI member would additionally need to provide Robust Notice at the point of PII collection.

An NAI member acting purely as a service provider to an advertiser client may continue to engage in Audience-Matched Advertising on behalf of that client, even in the presence of an opt out linked to a user’s PII, if the user has permitted Audience-Matched Advertising by the client by providing Opt-In Consent directly to that client.

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. 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.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 into interest segments such as “car enthusiast.” The same principle applies to data collection through applications on devices, as covered by Cross-App Advertising.

⁶ See FTC Final Privacy Report, *supra* note 4, at 42.

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.” 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 and the searches performed).⁷

TAILORED ADVERTISING

Tailored Advertising is a collective term for Interest-Based Advertising, Cross-App Advertising, Audience-Matched Advertising, Viewed Content Advertising, and Retargeting, as well as any combination of these activities. Consistent with the NAI’s approach to classifying digital advertising activities based on the point of data collection, data collected solely in a web browser is considered to be Interest-Based Advertising if it results in digital advertising in any of the media covered by the Code, and data collected solely on a television is considered Viewed Content Advertising under the same circumstances. The same principle applies to Cross-App Advertising and solely app-based data, as well as Audience-Matched Advertising and solely “offline” data.

On account of Cross-Device Linking, the NAI also recognizes that data collected in one medium can be linked with other data from another medium. In such cases, the data use becomes Tailored Advertising when used to target advertising through any medium covered by the Code. However, if data is based solely on one source, the NAI will apply the Code requirements based on the source through which the data was collected. As such, if only application-based data is used to target an ad on a television, it would be considered as Cross-App Advertising. Conversely, if only Viewed Content Information is used to target an ad on a mobile device, it would be considered Viewed Content Advertising. Tailored Advertising does not include Ad Delivery and Reporting, unless the resulting data is later used to tailor advertising, rendering it no longer Ad Delivery and Reporting.

Further, the NAI intends to cover any use of previously-collected user-level data to target a digital advertisement, whether that data was originally collected by the member, a third-party, or an advertiser. Thus, if an NAI member uses such data to participate in the tailoring of a digital advertisement in a medium covered by the Code, even if not explicitly mentioned here, it is the NAI’s intention that the NAI member take steps to abide with all of the provisions herein as they apply to Tailored Advertising as a means of “future-proofing” consumer notice and choice when it comes to such activities.

PII, DII, AND DE-IDENTIFIED INFORMATION

As stated in the introduction to the Code, the Code divides data into three categories based on the identifiers that it is tied to: Personally-Identified Information (PII), Device-Identified Information (DII), and De-Identified Information.

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

- Data that is linked or intended to be linked to a *directly identified individual* is considered PII.
- Data that is linked or intended to be linked to a *specific browser or device* is considered DII.
- Data that is not linked or intended to be linked to either an individual or to a specific browser or device is considered De-Identified Information.

⁷ See FTC Final Privacy Report, *supra* note 4, 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).

The NAI believes that it is appropriate for the Code to continue to encourage data minimization among its members for Tailored Advertising purposes. Accordingly, 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.

PII

PII includes any information linked or intended to be linked to an identified 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 Tailored 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.

The Code requirements that apply to PII apply equally to any data or data sets tied to PII. For example, if demographic information (e.g., age, gender), which would typically be considered DII when linked to a browser or device, 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.

In shifting its terminology from *Personally-Identifiable* to *Personally-Identified* the NAI acknowledges that with enough time, effort, and resources many data points that are traditionally tied only to a device can likely be linked to an identifiable individual. Thus, the NAI definition of PII shifts away from what one may hypothetically do with the data and moves to address what a given company publicly pledges to do with the data. From the NAI’s perspective, it is more helpful to users for members to disclose the types of data they collect, and how they use that data, than it is to provide a blanket statement that in theory, with enough resources, most data could be linked to a directly identified individual. The former approach allows users to make choices regarding whether to share data with an NAI member based on how a company promises to treat such data.

Hashed PII such as an email address is not considered to be PII if used only in its one-way encrypted form as a means of linking devices for Cross-Device Linking or matching audiences for Audience-Matched Advertising, and if no data collected through Tailored Advertising is linked to an unencrypted or un-hashed form of the PII.

DII

DII is defined as “data that is linked or intended to be linked to a particular browser 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. Effectively, the use of DII enables NAI members to collect and use data in a pseudonymous manner by tying certain interests or inferences to a specific, but unknown, user. DII does not include De-Identified Information.

Examples of how a member company may help ensure that the data it collects and uses for Tailored Advertising 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 other 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 Tailored Advertising purposes.

De-Identified Information

The Code defines De-Identified Information as “data that is not linked, or intended to be linked to an individual, browser, or device.” Data would be considered “De-Identified Information” 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 re-associated or 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 address), or truncating such identifiers; (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 other entity that receives the De-Identified Information 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 Information 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.⁸

Under the definition of De-Identified Information, the NAI Code refers to both group data and certain individual data. First, De-Identified Information 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 Information.

Second, De-Identified Information 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, 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.

OPT-IN CONSENT

NAI members may obtain a user’s Opt-In Consent through a direct interaction in which the NAI member details the proposed uses for the data being collected, requiring the user to perform an affirmative action as a manifestation of consent to the described use of the data.

Additionally, when NAI members are not in a position to interact directly with a user, they may obtain reasonable assurances of Opt-In Consent by relying on a partner engaged in a first-party interaction with the user to inform the user of the proposed uses of the data being collected as part of the consent process. Some methods through which NAI members may obtain reasonable assurances of Opt-In Consent are detailed below. If an NAI member wishes to rely on different means of obtaining reasonable assurances, these should be cleared with NAI staff to help ensure compliance with the Code.

Those NAI members who have a direct technical integration with a website or application, such as through a Software Development Kit (SDK), shall take steps to include such functionality that would enable the website or application to provide just-in-time notice, such as through an interstitial page, prior to the use of platform-provided consent mechanisms. These NAI members shall also take steps to contractually require the website or application to provide just-in-time interstitial notice prior to the use of platform-provided consent mechanisms or to provide more detailed messaging in the platform consent dialog itself unless the website or application already provides such notice or messaging.

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

Those NAI members who do not have a direct technical integration with a website or application, but do have a direct contractual relationship with a website or application, shall take steps to contractually require that website or application to provide just-in-time interstitial notice prior to the use of platform-provided consent mechanisms or to provide more detailed messaging in the consent dialog itself.

Those NAI members who do not have a direct contractual relationship or a direct technical integration with a website or application, and instead receive data via third-party intermediaries, including through bid requests, shall take steps to ensure that the third party, in turn, contractually requires its partner websites or applications to provide just-in-time interstitial notice prior to the use of platform-provided consent mechanisms or to provide more detailed messaging in the consent dialog itself.

When relying on contractual measures to ensure that additional notice is provided to users at the time of consent, NAI members shall take reasonable steps to confirm that such notice is provided. This may be accomplished by reviewing all or a representative sample of websites and/or applications from which the member receives the type of data in question.

PRECISE LOCATION INFORMATION

The definition of Precise Location Information is meant to recognize that a range of technologies may be able to provide members, “with reasonable specificity,” the actual physical location of a user or device. 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.⁹

Accordingly, the definition of Precise Location Information 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.¹⁰

The definition of Precise Location Information also does not include location data that has been altered prior to its provision for use in Tailored Advertising or Ad Delivery and Reporting, so that a member is unable to determine with reasonable specificity the actual physical location of a user or device. For example, a member will not be deemed to be using Precise Location Information 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 Tailored Advertising or Ad Delivery and Reporting. Importantly, using Precise Location Information in real-time, such as in geo-fencing, requires Opt-In Consent or Reasonable Assurances that an application or website has obtained such consent on behalf of the member, unless the data has been rendered imprecise prior to its use. Precise Location Information 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 Information.

⁹ See Guidance for NAI Members: Determining Whether Location is Imprecise, available at https://www.networkadvertising.org/sites/default/files/nai_impreciselocation.pdf.

¹⁰ These examples are provided in this Code for illustrative purposes only.

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.¹¹

ROBUST NOTICE

NAI members are required to provide Robust Notice when using PII, or merging PII with DII collected on unaffiliated websites or applications, or from covered devices, for Tailored Advertising purposes on a going-forward basis.

Such notice must be clear and conspicuous, which may vary with the complexity and style of the web page, application, or interface, as well as the size of the screen on which the notice must appear. Robust Notice must be provided at the time and place of the initial collection of data for Tailored Advertising. The notice must be located directly adjacent to the PII entry field or submit button. For online data collection, Robust Notice is only valid when the user engages a submit button or otherwise affirmatively confirms that they wish to submit the data to the recipient. Consequently, a user's email address may only be collected for the given purposes if that user has clicked on a submit button, rather than simply entering the email address in a given field and not having indicated an intention to submit such data.

Robust Notice shall disclose the intended use of the data, including merger with other data collected on unaffiliated websites, or applications, or on covered devices, for Tailored Advertising purposes. If the data is to be collected or used on multiple devices for Tailored Advertising, the notice must also disclose Cross-Device Linking.

The content of the notice may vary based on the nature of the collected data and its uses. When collecting data directly from a user, an advertiser relying on an NAI member strictly as a service provider for Tailored Advertising purposes on behalf of that advertiser, may inform the user that the data will be used in accordance with the advertiser's terms of service or privacy policy. However, if collecting data from a user that will be shared with third parties who may retain individual rights to such data for their own Tailored Advertising purposes, Robust Notice shall also include additional details regarding the sharing practices and uses permitted by the party collecting the data. The NAI will provide "mock-ups" on its website to further clarify expectations for the location and content of Robust Notice.

¹¹ 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>.

SENSITIVE INFORMATION

Health

The definition of Sensitive Information 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 Information for Tailored Advertising or Ad Delivery and Reporting requires Opt-In Consent from users.

First, Sensitive Information 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 Tailored Advertising or Ad Delivery and Reporting that triggers the requirement for Opt-In Consent, regardless of which health or medical condition the segment references.

Second, Tailored Advertising (whether through “standard” interest segments, custom segments, or Retargeting) or Ad Delivery and Reporting 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” information in the health space because whether a particular condition is considered sensitive may depend on the affected user 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.”¹² 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, all conditions predominantly affecting or associated with children that are not treated by over-the-counter medications, 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 general wellness topics that do not 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.

¹² 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.

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 Tailored Advertising or Ad Delivery and Reporting involving a sensitive health condition that NAI staff determines meets the criteria outlined here, subject to all procedures 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 the interest segments they use for Tailored 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, *infra* p. 26).

These restrictions are not intended to apply to interest segments designed for fundraising and similar non-profit uses, so long as those segments are not based on inferences that a user is likely to have a particular condition, but rather that users are likely to donate to charitable causes such as medical research or medical facilities. Such segments may not be used to target advertising for treatments or medications.

Similarly, Tailored Advertising aimed at medical professionals who may specialize in the treatment of sensitive conditions does not require a user’s Opt-In Consent as no inference is made that such a user may have a sensitive condition.

Restrictions on the use of Sensitive Information for Ad Delivery and Reporting are not intended to limit contextual advertising campaigns on websites or applications that address sensitive topics or general measurement and reporting regarding such campaigns. Rather, NAI members must obtain a user’s Opt-In Consent in order to use audience segments involving Sensitive Information for reporting purposes, as well as to target users at potentially sensitive locations, such as abortion clinics or LGBT clubs, using real-time Precise Location Information.

Sexual Orientation

The Code prohibits companies from collecting or storing information, including inferences, about a user’s status or perceived status as gay, lesbian, bisexual, transgendered, or gender non-conforming, for Tailored Advertising or Ad Delivery and Reporting without obtaining Opt-In Consent. The Code does not intend to prohibit targeting 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 “LGBT” as well as the Retargeting of visitors to sites that reflect the user’s sexual orientation, such as dating or travel sites *targeted specifically to LGBT visitors* without affirmative Opt-In Consent. 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 Tailored Advertising or Ad Delivery and Reporting.

These restrictions are not intended to apply to interest segments designed for political causes, so long as those segments are not based on inferences that a user’s status is gay, lesbian, bisexual, transgendered, or gender non-conforming, but rather that the user is likely to vote in favor of or support LGBT-related political causes. Such segments may not be used to target advertising for LGBT products, services, or websites.

SENSOR INFORMATION

Sensor Information is defined to include information from a camera, microphone, or any sensor on a user's device that may collect biometric data from such device. NAI members using Sensor Information such as from a microphone or camera for Tailored Advertising or Ad Delivery and Reporting must obtain the user's Opt-In Consent.

However, restrictions on the use of Sensor Information do not include information such as accelerometer data that is used to determine the status of the device, for example whether it is lying with the screen down on a table, or in combination with barometric pressure and/or Precise Location Information to determine the device's location inside large structures.

VIEWED CONTENT INFORMATION AND VIEWED CONTENT ADVERTISING

Viewed Content Information is intended to refer to videos, titles, programs, or similar content viewed on a television. Identifying viewed content based on non-visual information, such as HTTP headers, URLs, or audio is included in this definition. Viewed Content Information refers to video, rather than static images, and does not extend to all internet-connected history. This means that Viewed Content Information includes videos, titles, programs, or similar content viewed on a television, but does not cover web-browsing data collected on a television. This approach is consistent with the NAI's treatment of web browser data on mobile devices, which falls under Interest-Based Advertising rather than Cross-App Advertising.

Viewed Content Advertising is a subset of Tailored Advertising and describes the activity of tailoring advertisements for particular televisions, households, browsers, or devices based on Viewed Content Information. Collection of all, or substantially all, Viewed Content Information from a television, such as through automated content recognition technology, requires a user's Opt-In Consent.

Member Requirements

EDUCATION (§ II.A)

Members shall use reasonable efforts to ensure that users are aware of Tailored Advertising, its benefits, and how data is collected and used for these purposes. In addition, members shall ensure that users are aware of NAI-supported choice mechanisms and have easy access to such mechanisms. Participation in NAI-commissioned Public Service Announcement campaigns through inventory donation, creative resource allocation, or other means can help members comply with this Code requirement.

Members may also fulfill this requirement by speaking at industry events, providing privacy-related information on publicly available websites, or contributing articles and blog posts to enhance awareness of Tailored Advertising practices and the choices available to users.

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 Tailored 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 covered 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. When providing data retention disclosures, members must approximate a finite timeframe for such retention of PII and DII, before the data is aggregated or otherwise de-identified. 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 Tailored 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 Tailored 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.

Members collecting Viewed Content Information directly from televisions for Tailored Advertising or Ad Delivery and Reporting should disclose this in their notice, along with words such as “television,” “TV,” or similar terms, as appropriate.

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 agrees 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. The NAI will work with members to standardize categories of data collected for Tailored Advertising if the disclosure of such categories may be required by state or federal law.

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 a user’s decision about whether to opt out of Tailored 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 Information that requires Opt-In Consent. Nonetheless, the use of such standard segments requires 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 shall disclose a representative sample of their health-related custom segments and Retargeting activities, or otherwise explain their use of health-related information for Tailored Advertising.

Members using both standard and custom interest segments shall provide a full list of all standard segments and a representative sample of custom segments.

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.

POLITICAL TRANSPARENCY REQUIREMENT (§ II.B.3)

The political transparency requirement is intended to address the shifting landscape and public perception regarding political advertising. The NAI acknowledges that political advertising may factor into a user’s decision about whether to opt out of Tailored Advertising by a particular member company. Member companies may seek to target users on the basis of general political sentiment, interest in specific political issues, or political party affiliation. The use of such standard segments requires disclosure under these 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 political interests or proclivities, members are expected to have internal policies governing any use of politically-related targeting. This requirement is not intended to capture all politically-related advertising, as sometimes non-political interests or affinities can be used as proxies for political sentiment. It is not the NAI’s intention for members to list any segment that could potentially lead to an inference about the user’s political views, such as “vegetarian,” “gun owner,” “or import car owner.” Rather, the NAI intends for its members to disclose direct political segments such as “Democrat,” “Republican,” or “Pro-Choice.”

Many NAI members do not use standard interest segments, but may engage in Retargeting or the creation of “custom” segments. In such cases, members shall instead disclose a representative sample of their politically-related custom segments and Retargeting activities, or otherwise explain their use of politically-related information for Tailored Advertising.

Members using both standard and custom interest segments shall provide a full list of all standard segments and a representative sample of custom segments.

WEBSITE AND APP STORE NOTICE (§ II.B.4-8)

Contractual Notice Requirements (§ II.B.4-6)

If an NAI member company has a direct contractual relationship with a website or application where it conducts Tailored Advertising, it shall take steps to contractually require the website or application to post notice of Tailored Advertising and a link to, or instructions for, accessing an Opt-Out Mechanism.¹³ 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, 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 Tailored 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. On televisions, such notice should be provided on the screen or user interface most appropriate in this context.

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

¹³ 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 Tailored 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 Tailored Advertising purposes.

reasonably-sized sample of the websites and applications where they conduct Tailored Advertising to ensure that the websites and applications provide appropriate notice, following up with those that do not.¹⁴

Enhanced Notice Requirement (§ II.B.8)

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 Tailored 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 Tailored Advertising is provided outside of the privacy policy or the terms of service of a webpage where the advertisement is served.

Because NAI members also adhere to the DAA Principles,¹⁵ the NAI expects them to follow DAA guidance regarding specific applications of enhanced notice, including that relating to targeted political advertising.¹⁶

The NAI recognizes that the provision of enhanced notice may not be possible in all media and environments, and that a framework for enhanced notice may not be available due to technical challenges, such as ad formats used by publishers that do not allow for external links. The NAI only intends to enforce the enhanced notice requirement when and where it is possible for a member to provide or support such notice. At the time of publication of this Code, the NAI will not enforce enhanced notice requirements with regard to Viewed Content Advertising as a framework does not yet exist for such notice directly on television sets.

In addition, if a publisher or advertiser asks an NAI member to conduct a campaign informed by Tailored Advertising without enhanced notice in a medium where such notice is typically provided, 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.

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 Tailored Advertising purposes. The Code also requires that members obtain Opt-In Consent for the collection and use of Precise Location Information, Sensitive Information, Sensor Information, and Personal Directory Information for Tailored Advertising and Ad Delivery and Reporting, as well as for the collection of all, or substantially all, Viewed Content Information from a television. For the use of PII or its merger with DII for Tailored Advertising purposes, the Code requires the provision of an Opt-Out Mechanism tied to such PII, coupled with Robust Notice.

¹⁴ 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 Tailored Advertising purposes only where they serve ads. Member companies that provide in-ad notice pursuant to Section II.B.8 and only collect data for Tailored Advertising purposes where they serve ads will ensure that notice is provided wherever they collect data for Tailored Advertising, and need not contractually require their partners to provide notice or enforce contractual notice requirements.

¹⁵ See DAA OBA Principles, *supra* note 1.

¹⁶ See Digital Advertising Alliance, Application of the Self-Regulatory Principles of Transparency & Accountability to Political Advertising, available at http://www.aboutpoliticalads.org/sites/politic/files/DAA_files/DAA_Self-Regulatory_Principles_for_Political_Advertising_May2018.pdf.

Choices Regarding Use of PII or Hashed PII for Tailored Advertising (§ II.C.3)

Members who use PII or hashed PII for Tailored Advertising, alone or in conjunction with DII, must provide a PII-based Opt-Out Mechanism for such use of the data.

An Opt-Out Mechanism for a member’s use of PII or hashed PII shall apply to the member’s use of that PII or hashed PII for Tailored Advertising on all browsers, applications, and devices and shall be made available on both the member’s website and on the NAI website. If an NAI member uses types of PII or hashed PII that are not supported by the NAI Opt-Out Mechanism, and are not linked to the types of PII or hashed PII supported by the NAI Opt-Out Mechanism, the member shall provide an Opt-Out Mechanism for such PII or hashed PII directly on the member’s site. PII or hashed PII collected through such an Opt-Out Mechanism may only be used by the member to maintain the user’s opt-out preference.

NAI members employing the services of a third party for the matching process of Audience-Matched Advertising must also contractually require the third-party service provider to offer an Opt-Out Mechanism linked to PII.

If PII is not hashed before its use for Tailored Advertising, or if an NAI member intends to re-identify users after engaging in Audience-Matched Advertising, the NAI member would additionally need to provide Robust Notice at the point of PII collection.

An NAI member acting purely as a service provider to an advertiser client, who does not retain any individual rights to the data processed on behalf of the client, may continue to engage in Audience-Matched Advertising on behalf of that client, even in the presence of an opt out linked to a user’s PII, if the client contractually represents that the user has permitted Audience-Matched Advertising by providing Opt-In Consent directly to that client.

Choices Regarding Cross-Device Linking (§ II.C.4)

In 2017 the NAI published, and began enforcement of, its Guidance regarding Cross-Device Linking.¹⁷ 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 Tailored Advertising by a member company, the member shall effectively remove that browser or device from a device “map” for Tailored Advertising purposes and shall cease collecting data on the browser or device for Tailored Advertising use on any browser or device known or inferred to be linked to the opted-out browser or device. Similarly, the member shall cease Tailored Advertising on the opted-out browser or device with data from any browser or device known or inferred to be linked to that browser or device. These requirements are in addition to any other Code requirements regarding Tailored 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.5)

Following an opt out, member companies must cease collecting and using data for Tailored Advertising purposes for that browser or device. 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 Tailored Advertising purposes, regardless of the future opt-out status of the browser or device, or the technology used for Tailored Advertising. For example, if a user opts out of Tailored Advertising on a browser, but a month later deletes the opt out cookie. Under the Code, any data

¹⁷ See Guidance for NAI Members: Cross-Device Linking, available at https://www.networkadvertising.org/pdfs/NAI_Cross_Device_Guidance.pdf.

collected by the member company on the opted out browser during the month the browser was opted out may not be used for Tailored Advertising, even after the opt-out choice is deleted. Of course, a user may always choose to have such data used for Tailored Advertising by providing the member company with express, affirmative consent.

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

While members may continue to collect and use data for purposes other than Tailored 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 Tailored 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 Tailored 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 Compliance and Enforcement Procedures even if the opt-out may otherwise comply with NAI Code requirements.

Technologies Used for Tailored Advertising (§ II.C.6)

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.¹⁸ 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 2017.¹⁹

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. 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.

¹⁸ 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>.

¹⁹ 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 Tailored Advertising specifically targeted to children under 16 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 Tailored 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.²⁰ 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, employment eligibility, education eligibility, or tenancy decisions, would be inconsistent with that context. These use limitations are not intended to prohibit the use of data for the common good, including purposes such as the provision of Amber Alerts or severe weather alerts, and the provision of limited data sets to the scientific community to enhance data models used for evacuation planning or city transportation planning.

Material Changes (§ II.D.3)

Generally, a “material” change for purposes of this provision will relate to the collection or use of PII for Tailored Advertising purposes or the merger of DII with PII when a member previously represented that it does not 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. 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 across non-affiliate websites or applications for Tailored 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 Tailored Advertising purposes, to merge such DII with PII held by the receiving party without obtaining the user’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.

²⁰ See White House Privacy Report, *supra* note 4, at 18 (encouraging companies engaged in online advertising to refrain from collecting, using, or disclosing data that may be used to make decisions regarding employment, credit, and insurance eligibility or similar matters that may have significant adverse consequences to consumers and noting that such uses are at odds with generating revenue and providing consumers with ads that they are more likely to find relevant).

ACCESS (§ II.F.1)

To foster transparency and control where PII is used for Tailored Advertising, the Code requires member companies to provide reasonable access to any PII and associated DII collected and used for Tailored Advertising purposes and to provide users with a method of requesting the deletion of their PII and any associated DII. Such a deletion request mechanism is additional to the PII-based Opt-Out Mechanism required by section II.C.3 of the Code if members use PII for Tailored Advertising. However, members may combine the two functions into one user choice tool that allows the user to both opt-out of Tailored Advertising and to request access to or the deletion of their PII. Any PII collected during this process may only be used by the member to maintain the user's opt-out and deletion preferences.

The Code does *not* require companies to provide access to DII that is *not* associated with PII. However, some NAI member companies provide users 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 when practicable.

RESPONSIBLE 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; and (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, commensurate with the sensitivity of the data that is retained. 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 DII under the Code (or any PII used for Tailored Advertising or Ad Delivery and Reporting purposes), only so long as is necessary to serve the purpose for which the data was collected, or to fulfill another legitimate business need. 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 such data, or to render it De-Identified Information by taking steps to ensure that it cannot reasonably be linked to a particular individual, computer, or device.



409 7th Street, NW, Suite 250, Washington, DC 20004

www.networkadvertising.org