

Guidance for NAI Members: Opt-In Consent

November 2019



www.networkadvertising.org

INTRODUCTION

The 2020 NAI Code of Conduct (Code) sets forth data collection and privacy standards and imposes notice, choice, accountability, data security, and use limitation requirements on NAI member companies. Prior versions of the Code required Opt-In Consent for the use of Precise Location Information, Sensitive Data (such as sexuality and certain health-related data), and Personal Directory Data for Interest Based Advertising (IBA).¹ The 2020 Code adds Sensor Data to the list of data that is deemed sensitive and therefore requires Opt-In Consent for its use for Tailored Advertising or Ad Delivery and Reporting (ADR) purposes.² The Code has also been updated to clarify that in order to satisfy Opt-In Consent for all data types that require Opt-In Consent, a user must “manifest the intent to opt in to an activity described in a clear and conspicuous notice.”³

This document offers member companies further guidance on how to satisfy the 2020 Code updates, including examples for meeting the “clear and conspicuous notice” standard that is required for the purposes of Opt-In Consent, as well as steps member companies may take in order to rely on reasonable assurances that another party has obtained Opt-In Consent on the member’s behalf.

APPLICATION OF THIS GUIDANCE TO THE NAI CODE OF CONDUCT

The Network Advertising Initiative (NAI) issues this “Guidance for NAI Members: Opt-In Consent” consistent with the NAI’s self-regulatory framework and the 2020 version of the Code. This Guidance is not an update or an amendment to the Code, nor is it an endorsement of any specific technology or business model. Rather, this Guidance provides examples of how Code requirements may be satisfied and elaborates on best practices.

While consistent with the Code and other NAI Guidance documents, this Guidance discusses only certain requirements of the Code that are particularly relevant. This Guidance addresses notice and choice requirements for data that requires Opt-In Consent for Tailored Advertising or ADR. This includes Precise Location Information, Sensitive Data (such as sexuality and certain health-related data), Sensor Data, Personal Directory Data, and any data that is specified in the Code as requiring Opt-In Consent.

The NAI recognizes that the digital advertising ecosystem is evolving and companies may be in the process of developing new technologies and business models. This Guidance is to be applied to the use of any data, used for Tailored Advertising or ADR, that requires Opt-In Consent under the Code. Because of members’ rapid innovation, this Guidance includes an Appendix section with technology-specific guidance. Guidance may be updated periodically, and NAI staff may evaluate members’ practices on a case-by-case basis.

1 See NETWORK ADVERTISING INITIATIVE, 2018 NAI CODE OF CONDUCT § II.C.1 (2018), http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf [hereinafter 2018 NAI CODE OF CONDUCT].

2 See NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT § II.C.1 (2020), https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf [hereinafter 2020 NAI CODE OF CONDUCT].

3 2020 NAI CODE OF CONDUCT §I.H.

APPLICABLE CODE REQUIREMENTS

Definitions

I.A.: AD DELIVERY AND REPORTING

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. Data collection and use for security and fraud prevention does not fall within the scope of the NAI Code, therefore are not considered ADR. 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 the NAI Code of Conduct.⁴

I.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.⁵

Commentary to the 2020 NAI Code of Conduct

OPT-IN CONSENT

NAI members may obtain a user's Opt-In Consent through a direct integration 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 uses 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.⁶

⁴ See 2020 NAI CODE OF CONDUCT §I.A.

⁵ See 2020 NAI CODE OF CONDUCT § I.H.

⁶ See 2020 NAI CODE OF CONDUCT app. at 20.

COMMENTARY

There are two expanded-upon requirements of the 2020 Code that affect member companies' practices when using data in a category that requires Opt-In Consent. Additionally, this document provides guidance on segments created from data obtained through Opt-In Consent. This document addresses the following:

- A. Opt-In Consent requires "clear and conspicuous notice"⁷
- B. "Reasonable assurances" now requires additional contractual obligations⁸
- C. The creation of segments from certain types of data is considered a use of the data, which requires Opt-In Consent

These changes are intended to provide users with additional information that may be useful in making an informed choice about whether to allow or disallow certain types of data collection and use. Consistent with the Code, members shall retain opted in data collected for use in Tailored Advertising or ADR only as long as it is necessary for the purpose for which the data was collected, to fulfill another legitimate business need, or as required by law.⁹

A. Opt-In Consent Requires "Clear and Conspicuous Notice"

The Code requires that a member obtain a user's Opt-In Consent for the use of Precise Location Information, Sensitive Data (such as sexuality and certain health-related data), Sensor Data, and Personal Directory Data for Tailored Advertising or ADR. While historically, member companies have primarily satisfied this requirement through a technical integration or reasonable assurances that partners have obtained such consent on the member's behalf, the NAI had not elaborated on what constituted such reasonable assurances of Opt-In Consent, and instead pointed members to the Digital Advertising Alliance guidance on this topic.¹⁰

In the 2020 Code, the NAI clarified that Opt-In Consent has been updated to require "clear and conspicuous notice" which the Commentary describes as "detail[ing] the proposed uses of the data" that result in an "affirmative action as a manifestation of consent to the described use of the data."¹¹ The Commentary then goes to state that this notice should take the form of a detailed just-in-time notice, or interstitial, that is provided prior to the use of platform-provided consent mechanisms.¹² The NAI's goal with this notice requirement is to ensure that a user is presented detailed notice of the uses of data prior to, not after, making a choice.

⁷ See 2020 NAI CODE OF CONDUCT § I.H.

⁸ See 2020 NAI CODE OF CONDUCT app. at 20. The Code commentary also allows for methods beyond what is described in the commentary, however this must first be cleared by NAI staff to help ensure compliance with the Code.

⁹ See 2020 NAI CODE OF CONDUCT § II.F.4.

¹⁰ See DAA Application of Self-Regulatory Principles to the Mobile Environment at 29.

¹¹ 2020 NAI CODE OF CONDUCT app. at 20.

¹² A just-in-time notice is a notice presented at the time in which a user makes their choice. A common example of a just-in-time notice is an interstitial within an app for Precise Location Information. This just-in-time notice may be separate from the operating system's request to access location, and allows the user to make a choice about whether to let the application to access their location. For Precise Location Information, use cases we have seen have involved mobile applications. While this guidance discusses Precise Location Information specifically, the principle of requiring additional notice about the use of data should be applied to other instances of Opt-In Consent as required by the NAI Code. Please refer to the Commentary's section on Opt-In Consent for further details.

The following sections enumerate the detailed information that should be presented to users to serve as “clear and conspicuous” notice. A “clear and conspicuous” notice will include a description of purposes and a description of sharing practices.

I. DESCRIPTION OF PURPOSES

The NAI Code calls for users to receive just-in-time notice, or another form of notice at the time they initially provide consent, in order for an NAI member to reliably obtain Opt-In Consent or reasonable assurances that such consent has been obtained on the member’s behalf. This notice should (1) state that the data may be used for advertising activities and (2) characterize these activities with adequate specificity, such as listing the potential advertising uses of the data (Tailored Advertising, Attribution, and/or Analytics).

If a member company engages in Tailored Advertising, the NAI recommends describing the targeting of advertisements based on previously collected user data as Tailored Advertising.¹³ If a member company engages in ADR as described in the Code, the NAI recommends using more specific terms, such as Attribution and Analytics, as appropriate to describe their practices.

Members may wish to disclose these activities separately because users may be better able to make an informed decision based on whether the data collected will result in Tailored Advertising or if it will be used only for Analytics or Attribution.

Analytics means tracking advertisements to determine impacts of the advertising, the effectiveness of the targeting, and the quality of the creative. This may include measurement, determining demographics, segmenting, engagement, etc. Analytics may also include using data for research and commercial purposes in other industries such as finance, consulting, urban planning, and real estate. Attribution means engaging in activities, strategies, or the use of technologies to quantify the influence of an advertising impression. This allows marketers to optimize media spend for conversions and target advertisements with better accuracy.

A company can choose to be more specific, but the NAI suggests that short-form notice should not be overly complicated, and that members should attempt to use standard terminology to describe practices to better enable informed choice and provide users with a consistent experience.

¹³ 2020 NAI CODE OF CONDUCT § I.Q. 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 ADR, including, but not limited to, frequency capping or sequencing of advertising creatives.

II. DESCRIPTION OF SHARING PRACTICES

In describing how data that requires Opt-In Consent may be shared for Tailored Advertising and/or ADR purposes, NAI member companies should ensure that notice accompanying such consent states whether data sharing may occur and the categories of parties the data may be shared with. NAI recommends a multilayered approach with general disclosure in the just-in-time notice and a more detailed disclosure in the privacy policy.

Just-in-Time Notice

When detailed messaging is presented to a user about the collection and use of data, such as in an interstitial occurring prior to the use of a consent mechanism, members should ensure that such messaging explicitly states that the data may be shared with partners when such a possibility exists. Member companies that have direct technical integrations, such as a Software Development Kit (SDK), should include the functionality to provide such notice as part of the technical integration. Publishers can be more specific in notices, but member companies should take reasonable steps to ensure that publishers, at a minimum, provide the above notice.

Privacy Policies

After detailed messaging is presented to a user (such as in the form of a just-in-time interstitial notice), the user should have an opportunity to visit a website or mobile application publisher's privacy policy and receive the same, if not more detailed, information. This information is material to a user's choice to opt in to such uses.

Privacy policies should provide users additional information on categories of partners with which data will be shared.¹⁴ The category of partners does not need to specifically list the lines of business, or the names, of the companies. Rather, it is sufficient to disclose that opted in data may be shared with "Advertising Technology Companies." This term encompasses the lines of business and activities performed by NAI member companies.¹⁵

If an NAI member shares data obtained with Opt-In Consent with its partners, it should disclose the categories of partners in its own privacy policy. If an NAI member relies on contractual relationships with partners to obtain Opt-In Consent for the use of data, the contractual language should require that websites or applications include, in their privacy policies, categories of parties with whom they share the opted in data.

¹⁴ The CCPA requires businesses to disclose the categories of third parties with whom the business shares or discloses PI. See CAL. CIV. CODE § 1798.110(c)(4). The NAI's role is limited to providing guidance on the scope of the NAI Code; it does not offer legal advice on the CCPA nor is there guidance from the office of the California AG at the time of the publication of this document regarding the level of required specificity for disclosures of the categories of parties with whom data is shared.

¹⁵ The members, or the partners of members, can label the categories of parties with whom they share data with more specificity than the NAI requires. For example, "Location Intelligence," "Ad Network," "Ad Exchange," and "Data Management Platform" are examples of specific lines of business that could be disclosed but that level of specificity is not required under the NAI interpretation of the Code.

B. “Reasonable Assurances” Now Requires Additional Contractual Obligations

Where a company does not have a direct integration with a publisher and cannot itself obtain the Opt-In Consent, the Code requires that a member company receive reasonable assurances that Opt-In Consent has been obtained on its behalf. The NAI’s Opt-In Consent requirement helps ensure that companies that are unable to directly obtain Opt-In Consent can do so through contractual measures or other means.

Historically, some member companies have satisfied their existing NAI Code obligation to obtain reasonable assurances for the collection and use of opted in data, such as Precise Location Information, by relying on partners that have a direct technical integration with a mobile application through an SDK. Alternatively, when a member company does not receive the data from a partner that has a direct technical integration, but rather through an exchange bidstream, that company has had to obtain other reasonable assurances that Opt-In Consent has been provided.

In this section, the NAI elaborates on contractual or other measures members should take with partners who obtain Opt-In Consent on behalf of member companies. NAI member companies may obtain reasonable assurances of Opt-In Consent through:

- Contractual obligations that adequately describe the purposes and data sharing practices as described in this guidance
- Additional technical measures to ensure the presence of purpose and data sharing disclosures and to verify user choice

The Code Commentary allows for methods beyond contractual requirements to obtain reasonable assurances, with guidance from NAI staff to help ensure compliance with the Code.¹⁶

I. CONTRACTUAL OBLIGATIONS THAT ADEQUATELY DESCRIBE THE PURPOSES AND DATA SHARING PRACTICES AS DESCRIBED IN THIS GUIDANCE

As previously mentioned, many NAI members rely on contractual measures with partners if the member does not directly obtain Opt-In Consent.

Members may have direct technical integrations that do not rely on an SDK. In those instances, where data is transferred through batch server to server transfers that can occur at various frequencies (daily, weekly, etc.), members would need to rely on contractual measures if they do not have the capacity to provide real-time notice to users.

Many NAI members are not in a position to interact directly with a user. Members that have a direct contractual relationship with a website or application shall take steps to contractually require that website or application provide a just-in time interstitial notice or message with a level of detail that addresses the intended purposes and sharing of the data.¹⁷

¹⁶ “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.” 2020 NAI CODE OF CONDUCT app. at 20.

¹⁷ See *id.* at 20.

Members that do not have a direct contractual relationship or a direct technical integration with a website or application, and 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 or messaging in the consent dialogue itself with the level of detail regarding purposes and sharing as described in this document.¹⁸

Note that members who have a direct technical integration with a website or application, such as through a SDK, and who take steps to enable the website or application to provide just-in-time notice, shall also take steps to contractually require the website or application to provide the just-in-time interstitial notice prior to the use of platform-provided consent mechanisms or to provide more detailed messaging in the platform consent dialogue itself unless the website or application already provides such notice or messaging.¹⁹

The Commentary to the Code recommends that, in addition to relying on contracts, members take steps to ensure that such notice is provided. Steps may include reviewing all, or a representative sample of, websites and/or applications from which the member receives the type of data in question. Steps that members can take to ensure such notice is provided also include technical measures, as described in the following section.

II. ADDITIONAL TECHNICAL MEASURES TO ENSURE THE PRESENCE OF PURPOSE AND DATA SHARING DISCLOSURES AND TO VERIFY USER CHOICE

There are several methods the NAI recognizes for passing information through the bid stream to signal the presence of purpose, data sharing disclosures, and user choice. Technical measures can be taken by member companies to obtain reasonable assurances of Opt-In Consent. Beyond compliance with the NAI Code, implementing technical measures that provide reasonable assurances of Opt-In Consent may assist members in meeting their compliance obligations with respect to other laws and regulations. The NAI does not support or certify one method over another. However, companies with the means to implement technical measures should do so. By implementing technical measures (as described below) to pass signals, companies will be creating a more auditable and reviewable consent record. With this improved accountability, companies can demonstrate that they have obtained consented data and that their processing is consistent with the consent obtained.

In any technical means of passing or verifying consent for opted in data, such as Precise Location Information, the NAI recommends including, at minimum, certain information in the consent record.²⁰ The data types that should be included are:

- Device Level Identifier, e.g. Mobile Advertising ID
- Date/Time Stamp
- Source (App/Site Managing Consent Flow)
- Purposes by Party
- Consent Language
- Expiration Date

¹⁸ See *id.* at 21.

¹⁹ See *id.* at 20.

²⁰ Publishers can include additional signals such as whether adequate disclosures (not required by this document) have been offered.

In this list of data types, “Purposes by Party” would include the purposes previously mentioned in this document: Tailored Advertising, Attribution, and Analytics. These purposes would be specifically directed at the use of the opted in data. The disclosure that Precise Location Information, for example, will be shared with partners can either be included in “Purposes by Party” or it can be its own column in the consent record. “Consent Language” should include the choice (Opt-In) of a consumer for the use of the data for the purposes listed.

Current solutions may include adding columns to consent records specifically related to opted in data. For example, companies may update daily feeds that mobile companies receive from publishers, update the Open RTB spec, implement specifications that have been adopted in other jurisdictions such as the European Union (like the Transparency and Consent Framework), or use other methods.

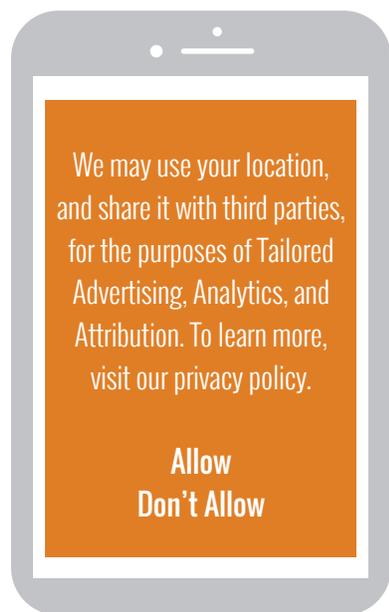
The NAI is agnostic on which method a member company implements to pass these signals. Rather, the NAI acknowledges that there are several technical solutions and companies may not all implement the same solution. NAI staff will, however, consider any implementation of a technical solution that follows this guidance to be a proactive effort on the part of the member company to strengthen the relationship between a user’s choice and how a user’s data is used.

C. The Creation of Segments from Certain Types of Data is Considered a Use of the Data, Which Requires Opt-In Consent

If any opted in data, such as Precise Location Information, Sensitive Data (such as sexuality and certain health-related data), Sensor Data, and Personal Directory Data, is received by a member company in raw form, such data requires Opt-In Consent, whether or not it is made imprecise, upleveled, used for modeling, or used for segmenting. In the case of Precise Location Information, for example, if a member receives latitude and longitude, any real time use, segmenting, or modeling, of that data will be considered a use by the NAI and will require Opt-In Consent. This applies to segmenting of any of the aforementioned data types. Members that do not receive the raw form of the data and receive the segmented or imprecise data would not need Opt-In Consent.

APPENDIX A: SAMPLE LANGUAGE

Sample of Interstitial



Sample of Contract Language

FOR CONTRACTS DIRECTLY WITH PUBLISHERS:

1. Partner [_____] shall obtain Opt-In Consent for the use of the following data: [_____]
2. Partner [_____] shall disclose to the user, prior to obtaining consent, the purposes for which data may be used, in an interstitial or just-in-time notice. Such purposes may include Tailored Advertising, Analytics, and Attribution, as applicable.
3. Partner [_____] shall disclose, in the interstitial or just-in-time notice, the sharing of data with partners or third parties.
4. Partner [_____] shall disclose, in its privacy policy, categories of third parties with which opted in data will be shared.

FOR CONTRACTS WITH THIRD PARTIES:

1. Partner [_____] shall contractually require the company from which it receives data to obtain Opt-In Consent for the use of the following data: [_____]
2. Partner [_____] shall contractually require the company from which it receives data to disclose to the user, prior to obtaining consent, the purposes for which data may be used, in an interstitial or just-in-time notice. Such purposes may include Tailored Advertising, Analytics, and Attribution, as applicable.
3. Partner [_____] shall contractually require the company from which it receives data to disclose, in the interstitial or just-in-time notice, the sharing of data with partners and third parties.
4. Partner [_____] shall disclose, and contractually require the company from which it receives data to disclose, in privacy policies, categories of third parties with which opted in data will be shared.

APPENDIX B: OPT-IN CONSENT FOR PRECISE LOCATION INFORMATION

I. Introduction

Protections related to Precise Location Information have been a key element of the NAI Code since the original self-regulatory principles in 2000. In previous versions of the Code, there had been an Opt-In standard for the use of Precise Location Information for Interest Based Advertising (IBA). Along with the updates and clarifications made in this document about how to satisfy NAI’s Opt-In requirement, this Appendix discusses additional updates to the 2020 Code in relation to Precise Location Information.

The 2020 Code updates the definition of Ad Delivery and Reporting (ADR) to now include the real time use of Precise Location Information and specifies that the use of Precise Location Information for ADR now requires Opt-In Consent.

In addition to the guidance given in Guidance to NAI Members: Opt-In Consent, member companies should refer to this Appendix for guidance on practices related to Precise Location Information. Additional guidance may be provided by NAI staff at any time and this document may be updated to reflect changes in the Code or best practices.

II. Applicable Code Requirements

II.C(1)(A): Use of Precise Location Information for Tailored Advertising or Ad Delivery and Reporting purposes shall require a user’s Opt-In Consent.²¹

I.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.²²

III. Commentary

Opt-In Consent is required for the use of Precise Location Information for Tailored Advertising or ADR. This document addresses the 2020 Code update to requirements around Precise Location Information:

In previous versions of the NAI Code, the Opt-In Consent requirement for the use of Precise Location Information applied only for Tailored Advertising. The 2020 update to the Code expands the scope to ADR. In this document, ADR is broken up into Analytics and Attribution. For both of those practices, Opt-In Consent is required. If a member company uses Precise Location Information for ADR, the NAI will expect for that company to obtain Opt-In Consent or reasonable assurances of Opt-In Consent through contractual measures and the NAI highly encourages members to pursue additional technical measures.

²¹ 2020 NAI CODE OF CONDUCT § II.C.1.g.

²² 2020 NAI CODE OF CONDUCT § I.L.

Additionally, in previous versions of the Code, if a member company did not store Precise Location Information, the member company could use Precise Location Information in real time without obtaining a user's Opt-In Consent. The 2020 Code changes this and subjects the use of Precise Location Information in real time to the Opt-In Consent requirement.

Members have been guided by the NAI's Imprecise Location Guidance to determine how to up-level or make imprecise their Precise Location Information before using or storing.²³ That document offers methodology by which data can be rendered imprecise. We continue to recommend that members implement technologically reasonable data minimization practices. Please refer to that document for more detail on what constitutes imprecise location data.

²³ NETWORK ADVERTISING INITIATIVE, GUIDANCE FOR NAI MEMBERS: DETERMINING WHETHER LOCATION IS IMPRECISE (July 20, 2015), https://www.networkadvertising.org/sites/default/files/nai_impreciselocation.pdf.