Best Practices:

Using Information Collected for Tailored Advertising or Ad Delivery and Reporting for Non-Marketing Purposes

June 2020

NAI
Network Advertising Initiative

www.networkadvertising.org

INTRODUCTION

The purpose of the NAI Code of Conduct (NAI Code) and the NAI's accompanying accountability program is to ensure that when NAI members process information for Tailored Advertising or Ad Delivery and Reporting (ADR), consumers have adequate privacy protections in connection with those practices, and NAI members have clear guidelines about how to implement those protections. In limited circumstances, those privacy protections include a prohibition on non-marketing uses of information collected as a result of Tailored Advertising or ADR due to the potential for consumer harm. Specifically, the NAI Code prohibits the use of that data for any non-marketing eligibility purposes, including employment eligibility; credit eligibility; health care eligibility; insurance eligibility, underwriting, or pricing; tenancy eligibility; and education admissions.[1]

However, the NAI recognizes that there are other legitimate, non-marketing uses for information collected for the purposes of Tailored Advertising or ADR that promise business and societal benefits. For example, a number of location intelligence companies in the NAI membership use information collected as a result of Tailored Advertising or ADR to provide valuable business analytics services that are not directly related to Tailored Advertising or ADR. Further, as the COVID-19 pandemic has revealed, information collected as a result of Tailored Advertising or ADR (and location data in particular) can be a valuable resource for the public good by helping researchers and policy-makers understand the spread of disease, the efficacy of social distancing measures, and other important insights. These non-marketing activities are not explicitly covered by the NAI Code, but there are still important privacy considerations NAI members should take into account when engaging in them. The best practices laid out here are intended to guide NAI member use of information, collected as a result of Tailored Advertising or ADR, for non-marketing purposes in a privacy-protective manner when those practices are not directly addressed by the NAI Code.

BEST PRACTICES

BEST PRACTICE 1

NAI Members should apply a materiality test to determine whether non-marketing uses of information collected for Tailored Advertising or ADR, particularly Sensitive Information,[2] should be explicitly disclosed.

The NAI Code is built around the principles of notice and choice. For those principles to provide effective privacy protections, users must have access not only to an effective choice mechanism, but also sufficiently relevant and detailed notice to enable them to make an informed choice. For example, the NAI Code includes more robust notice requirements that go hand-in-hand with heightened Opt-In Consent requirements for the use of information that requires Opt-In Consent for Tailored Advertising or ADR.[3] The NAI's *Guidance for NAI Members: Opt-In Consent* explains how to present users with a just-in-time notice that complies with the NAI Code. However, because Tailored Advertising, attribution, and analytics represent the predominant use cases that NAI member companies engage

1 Network Advertising Initiative, 2020 NAI Code of Conduct (Jan. 2020) (hereinafter "NAI Code") § II.D.2.

2 NAI Code § I.O.

3 Information that requires Opt-In Consent includes: Precise Location Information, Sensitive Information, Personal Directory Information, Sensor Information, collection of all or substantially all Viewed Content Information from a television for Viewed Content Advertising. NAI Code §§ II.C.1.d-i.

in, the NAI's Opt-In Consent Guidance was drafted with those use cases in mind. That is why it specifies that a just-in-time notice accompanying a request for a user's Opt-In Consent should disclose any use or sharing of relevant data for advertising, analytics, or attribution purposes.

Nonetheless, some NAI members and their partners engage in use cases that consumers may not easily understand to be advertising, attribution, or analytics. Some examples may be sharing for public health, business research, city planning, or even law enforcement purposes. When those use cases rely on information that requires Opt-In Consent (e.g., Precise Location Information, Sensor Information, or Sensitive Health Information), the NAI recommends including more detailed disclosures in the just-in-time notices that are already required for Tailored Advertising or ADR purposes. Specifically, when a business use case is (1) not easily understood as being advertising, attribution, or analytics; and (2) would likely be material to a consumer's choice to provide Opt-In Consent, the use case should be described separately in the just-in-time notice using a category that is intended to provide users with a meaningful understanding of the types of activities that the opted-in data may be used for, and, if applicable, the types of third parties it may be shared with.

Just-in-time interstitial notices should disclose proposed uses (purpose) and parties with whom the data will be shared. A company should consider materiality for each. The NAI follows the FTC's guidance on what constitutes a "material" consideration: The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service.[4] For example, if a contemplated use of location information may be to track movement of specific devices for "law enforcement purposes" or "research" (tracking unrelated to advertising, attribution, and analytics), then the company should apply a materiality test to determine whether that use of location information should be disclosed in just-in-time notice.

If the parties that the data will be shared with are ads-related companies, disclosing "third parties" or "partners" generally encompasses all of the ads-related companies. If a company has a government or law enforcement client who uses this data for ads-related reasons (analytics), the company should apply the materiality test to determine if it would be material to the user that the party is a government, and if so, disclose that in their just-in-time notice.

If a member company finds that it (or its partners) should update existing just-in-time notice language, that member company should refer to the *Guidance for NAI Members: Opt-In Consent* to see examples of notice and contract language.[5] As stated in the Opt-In Guidance, the NAI recommends the use of the terms "Tailored Advertising," "Attribution," and "Analytics" to describe ads-related practices that members may engage in. Members may choose to be more descriptive. For non-marketing practices, the NAI suggests the following terms, but recognizes that there are a variety of purposes that companies may also disclose:

- Research (e.g., business or investment research based on footfall data)
- Law Enforcement Purposes

4 *See* FTC Policy Statement on Deception (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

5 *See* Network Advertising Initiative, *Guidance for NAI Members: Opt-In Consent* 10 (Nov. 2019).

Disclosure of non-marketing uses and sharing, where applicable, should generally follow the parameters set forth in the NAI's Opt-In Consent Guidance. For example, such notice should be provided prior to the use of the platform-provided consent mechanism in a just-in-time or interstitial notice.[6] In this document, we provide several hypothetical scenarios that include examples of notice language based on different use cases. NAI members may also consider using other language that fits their specific use cases, but the language should sufficiently notify users about how information that requires Opt-In Consent will be used for non-marketing purposes or by non-commercial entities, as applicable. Note that these best practices recommend just-in-time notices to include two disclosures: a disclosure of proposed uses, and a disclosure of parties with whom data will be shared.

BEST PRACTICE 2

NAI members should use aggregate group data and/or de-identified user-level data wherever possible for non-marketing use cases.

In general, the use of aggregate and/or De-Identified Information mitigates privacy risks to individuals because such information does not pertain to an individual user or device. In recognition of that fact, the NAI Code has never imposed notice and choice requirements on NAI members in connection with their non-marketing uses of information collected as a result of Tailored Advertising or ADR. To further promote the privacy benefits of using aggregate or De-Identified information, NAI members who share information that requires Opt-In Consent for non-marketing uses should render it de-identified or aggregate it whenever possible, consistent with the purpose for sharing it. As discussed above, users are less likely to consider different uses of de-identified or aggregate information to be material to their choices about either providing Opt-In Consent or using an Opt-Out Mechanism, as applicable.

The NAI Code treats any De-Identified Information the same, whether aggregate or user-level[7] De-Identified Information. De-identified aggregate data refers to group-level data and de-identified user-level data refers to data that is stripped of individual identifiers but still distinguishable on an individual level (for example, hashed mobile advertising identifiers or pseudonymized data). For the purpose of this document, the NAI recognizes that de-identified user-level data, when based on location history, allows for a higher likelihood of potential re-identification. The NAI recommends treating de-identified user-level data as DII (Device Identifiable Information) and taking appropriate steps to provide notice upstream.

NAI members who share de-identified and/or aggregate information should also contractually prohibit reidentification of the information that requires Opt-In Consent by the receiving party or merger of the data with any other data that would identify a user or device.

6 *Id* at 4.

7 Examples of user-level data include, but are not limited to, Personally-Identified Information (PII), Device-Identified Information (DII), hashed PII, and other unique identifiers.

BEST PRACTICE 3

NAI members should extend some privacy protective NAI Code requirements to the use of information collected for Tailored Advertising or ADR for non-marketing purposes.

DATA MINIMIZATION

NAI members themselves may not retain information that is collected as a result of Tailored Advertising or ADR longer than necessary to achieve the purpose for which the data was collected, to fulfill another legitimate business need, or as required by law. Similarly, NAI members should limit such data that they share for non-marketing purposes to the minimum required to achieve the purpose it is shared for. In addition, NAI members should contractually require the recipients of such data to delete, de-identify, or aggregate user-level the data after the non-marketing purpose it was obtained for has been achieved, and set outer bounds with a finite retention period expressed in days or months. For example, if an NAI member shares user-level Precise Location Information with a public health authority to assist with contact tracing during a disease outbreak, it might require a retention period of no more than 90 days.

USE LIMITATIONS

NAI members should limit the use of information that is collected as a result of Tailored Advertising or ADR and that they share with recipients for non-marketing purposes to specified purposes identified in a written contract. For information that is collected as a result of Tailored Advertising or ADR and obtained pursuant to a user's Opt-In Consent, those purpose should be consistent with those disclosed in the just-in-time notice presented to the user in conjunction with the user's Opt-In Consent. For example, if an NAI member company shares Precise Location Information with an investment firm for purposes of understanding footfall for a retail client (i.e., "research"), the NAI member should ensure that any user-level Precise Location Information transferred for that purpose is properly permissioned (i.e. "research" was a disclosed purpose in the just-in-time notice required for Opt-In Consent), and include contractual restrictions on the further use of the information for law enforcement purposes if that purpose was not disclosed in the just-in-time notice.

TRANSFER RESTRICTIONS

NAI members should limit the downstream transfer of information that is collected as a result of Tailored Advertising or ADR by the intended recipient of the information. For example, if an NAI member shares information that is collected as a result of Tailored Advertising or ADR (for example, opted-in biometric sensor information or Precise Location Information) with a public health authority, the NAI member should include contractual restrictions on the transfer of that information to other entities, such as other government agencies.

REASONABLE SECURITY

NAI members must themselves use reasonable security measures to protect information that is collected as a result of Tailored Advertising or ADR, and should also pass that requirement by contract to downstream recipients of the data.

HYPOTHETICAL EXAMPLES DEMONSTRATING APPLICATION OF BEST PRACTICES

The below scenarios are based on a hypothetical NAI member company ("Member Company")[8] that provides location data services for advertising and other purposes. It has a software development kit (SDK) that allows it to integrate with partner mobile apps and collect Precise Location Information from a user's device when the user has installed a partner app and has given Opt-In Consent. Consistent with the NAI's Opt-In Consent Guidance, Member Company has included functionality in its SDK that allows partner mobile apps to surface a just-in-time notice to users explaining how Precise Location Information collected from their device will be used, and with whom it will be shared. Currently, the template notice used by Member Company consists of the following:

> **"We will collect and use location information for Tailored Advertising, Attribution, and Analytics, and will share this information with partners for those purposes."**

Member Company's partners have traditionally included other ad-tech companies, and its transactions with those companies are often covered directly by the NAI Code. However, Member Company has received inquiries and requests from both government and commercial clients regarding the use of Member Company's location information for various non-marketing purposes that would not be covered directly by the NAI Code. Therefore, Member Company should take into account the best practice considerations discussed above for the following transactions.

EXAMPLE 1

A financial services company is considering making an investment in a retail opportunity, but is seeking to evaluate the quality of the proposed location for the storefront based on pedestrian traffic nearby. The company wants to contract with Member Company to obtain user-level[9] Precise Location Information[10] to help it complete this evaluation. Member Company adopts the following best practices in connection with this transaction:

TRANSPARENCY

Member Company determines this use case is not advertising (or advertising-related attribution or analytics) and would be more easily understood by users as a form of "research." If Member Company accepts this contract, it determines it would need to alter its template notice as follows: "We will collect and use location information for Tailored Advertising, Attribution, Analytics, and **Research** and will share this information with partners for those purposes."

USE OF DE-IDENTIFIED OR AGGREGATE INFORMATION

Member Company discusses alternative solutions that do not rely on user-level data with its client to determine if they can meet the client's needs. In this case, Member Company discusses heat maps and relative traffic density statistics as alternatives to sharing user-level PLI.

---

8 These illustrative scenarios do not refer to, or represent, the activity of any actual NAI member company. Any resemblance to an actual company or use case is incidental.

9 Examples of user-level data include, but are not limited to, Personally-Identified Information (PII), Device-Identified Information (DII), hashed PII, and other unique identifiers. In these use cases, any reference to "user-level" data refers to data that has not been De-Identified. If the data at issue is user-level and De-Identified, the NAI recommends treating that data as DII, as discussed in this document.

10 Even when the location information the law enforcement agency receives has been rendered from Precise Location Information to imprecise, the Member Company is still obligated to present detailed notice of the proposes uses and sharing practices before Opt-In Consent is received.

OTHER PRIVACY-PROTECTIVE MEASURES

Member company includes contractual limitations as follows:

- Restricting secondary uses of PLI obtained from Member Company to those previously disclosed to end-users in a just-in-time notice.
- Setting a retention period or conditions for the PLI.
- Restricting downstream transfers of PLI shared with the financial services company to those categories of entities previously disclosed to end-users in a just-in-time notice.
- If any aggregate or deidentified information is shared, prohibitions on re-identifying or allowing downstream re-identification of such information.
- Requiring reasonable security measures for the disclosed information.

EXAMPLE 2

A state department of transportation wants to contract with Member Company to obtain user-level Precise Location Information to help it determine where to allocate budget resources for future infrastructure development and improvement projects. Member Company adopts the following best practices in connection with this transaction:

TRANSPARENCY

Member Company determines this use case is not advertising (or advertising-related attribution or analytics) and decides to label it "Research." Member Company also considers whether the receiving party being a state department of transportation is material for purposes of disclose in its just-in-time notice. If Member Company accepts this contract, it may alter its template notice as follows: "We will collect and use location information for Tailored Advertising, Attribution, Analytics, and **Research** and will share this information with partners for those purposes." Please note that Member Company should apply a materiality test to both the purpose and the party and disclosure may depend on the materiality of either or both of those factors. Member Company may determine in this hypothetical to disclose "governments" as a receiving party of the data if they find that "Research" does not sufficiently cover the proposed activity.

USE OF DE-IDENTIFIED OR AGGREGATE INFORMATION

Member Company discusses alternative solutions that do not rely on user-level data with the state department of transportation to determine if they can meet the client's needs.

OTHER PRIVACY-PROTECTIVE MEASURES

Member company includes contractual limitations as follows:

- Restricting secondary uses of PLI obtained from Member Company to those previously disclosed to end-users in a just-in-time notice (e.g., PLI shared with the state department of transportation may not be shared with another government agency for law enforcement purposes because law enforcement purposes were not disclosed in the just-in-time notice).
- Setting a retention period or conditions for the PLI.
- Restricting downstream transfers of PLI shared with the state department of transportation to those categories of entities previously disclosed to end-users in a just-in-time notice.
- If any aggregate or deidentified information is shared, prohibitions on re-identifying or allowing downstream re-identification of such information.
- Requiring reasonable security measures for the disclosed PLI.

EXAMPLE 3 A federal law enforcement agency wants to contract with Member Company to obtain user-level Precise Location Information so it can more effectively track the movements of mobile devices, allowing it to identify population trends, allocate surveillance resources, and to possibly generate and investigate leads relating to criminal activity.

TRANSPARENCY

Member Company determines that the purposes contemplated by this transaction are not advertising (or related advertising attribution or analytics). The fact that the information could be used for a law enforcement purposes instead of a commercial purpose is also likely to be material to users. If Member Company accepts this contract, it determines it would need to alter its template notice as follows: "We will collect and use location information for Tailored Advertising, Attribution, Analytics, **and for Law Enforcement purposes**, and will share this information with **partners, including government entities**, for those purposes."

USE OF DE-IDENTIFIED OR AGGREGATE INFORMATION

Member Company discusses alternative solutions that do not rely on user-level data with the federal law enforcement agency to determine if they can meet the client's needs.

OTHER PRIVACY-PROTECTIVE MEASURES

Member Company includes contractual limitations as follows:

- Restricting secondary uses of PLI obtained from Member Company to those previously disclosed to end-users in a just-in-time notice.
- Setting a retention period or retention conditions for the PLI.
- Restricting downstream transfers of PLI shared with the law enforcement agency to those categories of entities previously disclosed to end-users in a just-in-time notice.
- If any aggregate or deidentified information is shared, prohibitions on re-identifying or allowing downstream re-identification of such information.
- Requiring reasonable security measures for the disclosed PLI.

EXAMPLE 4 A public health authority is requesting location information from Member Company to track the spread of a potentially deadly virus during a pandemic. Member Company has an internal policy allowing the sharing of location information with government agencies or public health authorities in exigent circumstances, including circumstances that are likely to lead to death or serious bodily injury. Member Company determines that a pandemic is an exigent circumstance because it presents a risk of death to those that contract the virus.

TRANSPARENCY

Because this is an exigent circumstance, Member Company would not have to alter its template notice if it uses other privacy-protective best practices.

USE OF DE-IDENTIFIED OR AGGREGATE INFORMATION

Member Company discusses alternative solutions that do not rely on user-level data with the public health authority to determine if they can meet the exigent needs.

OTHER PRIVACY-PROTECTIVE MEASURES

Because sharing with public health authorities is for limited, exigent circumstances and is not separately disclosed in a just-in-time notice, Member Company includes enhanced contractual limitations as follows:

- Restricting any secondary uses of PLI obtained from Member Company by the public health authority.
- Setting a finite retention period for the PLI (e.g., 90 days) or when the purpose of the sharing is achieved, whichever is sooner.
- Restricting any downstream transfers of PLI shared with the public health authority.
- If any aggregate or deidentified information is shared, prohibitions on re-identifying such information.
- Requiring reasonable security measures for the disclosed PLI.

EXAMPLE 5 A state law enforcement agency serves Member Company with a valid search warrant requesting that it produce any location information Member Company has with certain date-time stamps within a 1000m radius of a set of latitude and longitude coordinates. Member Company meets its legal obligations by complying with the warrant. Member Company further determines that complying with mandatory legal process is not a separate purpose for which it collects Precise Location Information, and that extraction of location information through a warrant is not "sharing" with a third party over which it has control. Compliance with legal process does not entail any enhanced transparency or contractual limitations under these best practice recommendations. Neither this document, nor the NAI Code, are intended to serve as a basis for non-compliance with a lawful subpoena, warrant, or other court order.

Discussion of Hypothetical Scenarios

Variants of the hypothetical use cases described above may in some cases involve only aggregate or De-Identified Information. The NAI encourages the use of aggregate or De-Identified Information wherever possible, and the NAI Code does not impose notice and choice requirements on the use of De-Identified Information. However, the NAI strongly encourages members to be as transparent as possible (including through just-in-time notices or privacy policies) with respect to all information that may be material to user choice. Additionally, in this document, the NAI recommends treating de-identified user-level information as DII.

The NAI recognizes that its members may not always be in a position to know specifically how a government client intends to use Precise Location Information they provide. For example, in scenario #3 above, Member Company may not have known whether the federal law enforcement agency intended to use Member Company location information for law enforcement purposes (i.e., the detection or investigation of unlawful activity), or only for other purposes that may be adequately described as "research" (compare with the state department of transportation use case in scenario #2). If that is the case, and Member Company does not intend to include a more detailed just-in-time notice disclosing the detection of unlawful activity (or other law enforcement purposes) as a purpose of collection, Member Company should prohibit the use of its data for law enforcement purposes in its contract with the government agency, consistent with best practices described herein for use limitations. Alternatively, if Member Company does know that the agency intends to use Member Company data for law enforcement purpose, Member Company should include that fact in the just-in-time notice.

Member companies should carefully consider the hypothetical examples when developing internal policies and procedures for their own use or sharing of information collected as a result of Tailored Advertising or ADR for non-marketing purposes (if applicable), but these scenarios do not represent absolute conclusions by the NAI staff as to the materiality of the facts disclosed, or not disclosed, for actual use cases. Member companies in each case should undertake their own analysis as to the materiality of the purposes and parties at issue when crafting their just-in-time disclosures.

CONCLUSION

The NAI membership is comprised of technology and data companies that have chosen to participate in the strongest self-regulatory program for digital advertising activities, and have long been guided by the NAI Code's privacy-protective requirements for Tailored Advertising and ADR. However, as NAI members continue to innovate and find new uses of information collected as a result of Tailored Advertising or ADR, they should continue to look to the NAI Code as a guide for their activities that do not fall squarely under the ambit of the Code. The NAI staff hopes these best practice recommendations will assist NAI members in continuing to develop innovative uses of data and technology in a way that preserves user trust and privacy.