NAI
PRIVACY, ACCOUNTABILITY & TRUST

Network Advertising Initiative Principles & Self-Regulatory Framework

DECEMBER 2024

TABLE OF CONTENTS

I. Introduction

For 25 years, the Network Advertising Initiative (NAI) has promoted strong privacy practices among member companies engaged in Network Advertising (defined below). Historically, that has taken the form of member adherence to an NAI Code of Conduct with detailed, prescriptive requirements that defined member obligations in the absence of state or federal consumer privacy laws. However, as more U.S. states pass comprehensive consumer privacy laws, the NAI is adopting a different approach to self-regulation for Network Advertising that better aligns with new and emerging legal requirements in the U.S.

To address this paradigm shift in the U.S. toward comprehensive consumer privacy laws, the NAI's new approach to self-regulation (the "Framework") relies on a combination of high-level privacy principles that are binding on NAI member companies and set a baseline for what it means to be an NAI member company; as well as non-binding best practices, guidance, and tools designed to assist member companies in understanding and complying with their privacy obligations and commitments under the law. The NAI's accountability program will continue to support member adherence to the new NAI Framework. **The NAI Framework set forth in this document supersedes and replaces the 2020 NAI Code of Conduct.**

By relying on high-level principles as a foundation, the new NAI Framework is intended to be flexible and adaptable; and to allow the NAI and its member companies to more efficiently respond to the rapidly changing technological and legal landscape based on guidance and best practices aligned with state and federal laws and regulations without adding redundant requirements.

In summary, the new NAI Framework comprises the following elements:

- A set of high-level privacy Principles that NAI members must adhere to as part of their membership in the NAI.
- A suite of non-binding privacy best practices, guidance, and tools designed to assist NAI member companies in understanding and complying with their privacy obligations under U.S. law. These are intended to be adapted and modified as new laws and regulations are enacted to provide optional pathways for complying with applicable legal requirements as well as the NAI Principles. Certain existing NAI documents already support this model, and the NAI will continue to develop new documents through its working groups and task forces.
- Binding accountability requirements that each NAI member company must meet to demonstrate their adherence to the NAI Principles, which will be assessed by the NAI staff through annual privacy reviews and consultations. Although these accountability requirements are binding, they are designed to allow a level of flexibility and adaptability for implementation that aligns (and avoids conflict) with state privacy laws and other legal and regulatory requirements.

Additionally, it is important to specify what the new NAI Framework does **NOT** do:

- It is not another set of detailed, prescriptive self-regulatory compliance requirements for NAI members akin to the legacy NAI Code of Conduct.
- It does not specify methods NAI members must use to comply with legal requirements, nor guarantee compliance with legal requirements.

II. Scoping

These Principles apply to NAI members engaged in Network Advertising in the United States.

Network Advertising is data-driven, digital advertising involving interoperable exchanges of personal data used for or derived from the selection, delivery, and measurement of such advertising. It may include activities that support "sales," "shares," "cross-context behavioral advertising," "targeted advertising," or similar practices as defined by applicable laws in the United States. Network Advertising does not limit its scope to the use of particular technologies, and may be carried out via cookies, APIs, server-to-server transfers, privacy enhancing technologies, or other methods.

Network Advertising does not include digital advertising that is selected, delivered, and measured entirely by a single controller relying solely on personal data obtained or derived from the users of its owned-and-operated properties unless it involves exchanges of personal data. Additionally, Network Advertising does not cover a member's processing of personal data:

(1) for fraud prevention and/or security purposes;
(2) for purposes necessary to provide the services requested directly by the consumer; or
(3) concerning individuals acting in their capacity as that member's employee or representative.

III. Definitions [1]

The NAI has chosen not to provide specific definitions for the terms used in the Principles, unless otherwise noted. Providing NAI-specific definitions would require synthesizing sometimes disparate state law definitions of relevant terms, or else put the NAI in the position of making policy decisions about the best definitions for relevant terms that may not align with legal requirements – an approach the NAI is departing from after the 2020 Code of Conduct.

Still, the NAI Framework does use terms that correspond to those used in privacy laws and regulations in the U.S. and intends that their meaning align with the meaning assigned to them in applicable privacy laws and regulations as the context requires. Such terms include, but are not limited to:

A. "Personal Data" (in some states, referred to as "Personal Information")
B. "Consumer"
C. "Process" / "Processes" / "Processing"
D. "Control" / "Controls"
E. "Sensitive Personal Data" - in some states, referred to as "Sensitive Data" / "Sensitive Information" / "Sensitive Personal Information"

Nothing in the NAI Framework is, nor should it be taken as, legal advice regarding your compliance with any applicable laws or regulations. The NAI encourages all members to consult with their own legal counsel regarding compliance with laws and regulations in all geographic regions applicable to their business.

1 The NAI will engage in a review of its historical documents to help ensure that these terms are aligned with those used by the NAI in its member resources.

IV. NAI Principles for Privacy in Network Advertising

1. TRANSPARENCY

Each member company shall provide transparency into its processing of personal data.

2. CHOICE & CONSUMER CONTROL

Each member company shall offer consumers method(s) to signal a choice about how the company processes their personal data, for those activities which require choice under applicable laws.

3. DATA GOVERNANCE

Each member company shall take steps to ensure that its processing of personal data comports with its commitments and legal obligations.

4. SENSITIVE PERSONAL DATA

Each member company shall limit its processing of sensitive personal data to disclosed purposes, and purposes consented to by the consumer as required by applicable laws, and shall provide additional safeguards when processing such data.

5. ACCOUNTABILITY

Each member company shall demonstrate its alignment with its commitments and legal obligations tied to its processing of personal data.

V. Appendix A - Accountability Requirements for NAI Member Companies Under the Principles

1. Accountability Requirements for Principle 1 - Transparency

Principle: Each member company shall provide transparency into its processing of personal data.

NAI staff will review:

a. Whether each NAI member provides a publicly accessible notice on its website that describes the processing of personal data it controls ("Privacy Notice").
b. The content of the Privacy Notice and any additional public-facing disclosure(s) provided by the member.
c. Whether the Privacy Notice and any other disclosures (if provided) describe the member company's processing of personal data that it controls.
d. Whether there are any appropriate non-binding recommendations regarding other applicable best practices for transparency.

2. Accountability Requirements for Principle 2 - Choice and Consumer Control

Principle: Each member company shall offer consumers method(s) to signal a choice about how the company processes their personal data, for those activities which require choice under applicable laws.

NAI staff will review:

a. Whether each member company has a process in place describing how the member (1) provides and honors its own method(s) for consumers to signal choice directly to the member about its processing of personal data (e.g. cookie opt-out request tool, email opt-out request tool, etc.), and/or (2) honors a method other than one provided directly by the member for consumers to signal choices about the member's processing of personal data (e.g., platform flags, opt-out preference signals/universal opt-out mechanisms (such as Global Privacy Control signals).
b. The product and technology descriptions (and/or links and URLs leading to those descriptions) provided by the NAI member that involve processing consumer personal data controlled by the member for those activities which require choice under applicable laws.
c. Any links, URL(s), or other method(s) for accessing mechanisms (and content thereof) offered directly by the NAI member and enabling consumers to signal choices about the processing of personal data controlled by the member for those activities which require choice under applicable laws.
d. The links, URL(s), or other method(s) for accessing mechanisms (and content thereof) that the NAI member recognizes or honors (but not offered directly by the member) enabling consumers to signal choices about the processing of personal data controlled by the member for those activities which require choice under applicable laws.
e. Whether there are any appropriate non-binding recommendations regarding other applicable best practices for consumer choice and control.

3. Accountability Requirements for Principle 3 - Data Governance

Principle: Each member company shall take steps to ensure that its processing of personal data comports with its commitments and legal obligations.

NAI staff will review:

a. Whether each member company has implemented a written data governance program that addresses personal data processing across its organization. This program should cover, but is not limited to the following topics:
   i. How the member honors consumer opt-out requests it receives.
   ii. What processes the member has in place to respond to consumer requests in a timely fashion.
   iii. What steps the member takes to update disclosures to reflect new data processing.
   iv. What steps the member takes as part of its partner and vendor due diligence.

b. Whether there are any appropriate non-binding recommendations regarding other applicable best practices for data governance.

4. Accountability Requirements for Principle 4 - Sensitive Personal Data

Principle: Each member company shall limit its processing of sensitive personal data to disclosed purposes, and purposes consented to by the consumer as required by applicable laws, and shall provide additional safeguards when processing such data.

NAI staff will review:

a. Whether a member has implemented an internal policy that:
   i. Allows the member to assess whether personal data is sensitive.
   ii. Is designed to ensure that the member's processing of sensitive personal data is limited to legally permitted purposes, including, as applicable, purposes disclosed to or consented by the consumer.
   iii. Outlines additional safeguards the member has in place when processing sensitive personal data in those jurisdictions that place additional requirements around the processing of sensitive information.
   iv. Provides for regular risk assessments to identify and mitigate risks associated with the processing of sensitive personal data.

b. NAI staff may also review for and make non-binding recommendations regarding other applicable best practices for processing sensitive personal data.

5. Accountability Requirements for Principle 5 – Accountability

Principle: Each member company shall demonstrate its alignment with its commitments and legal obligations tied to its processing of personal data.

NAI staff will confirm that each NAI member has submitted responses to the NAI's annual privacy consultation questionnaire and met with NAI staff for an annual interview to discuss the questionnaire.

VI. Appendix B - Applicable Guidance, Best Practices, Tools, and Standards

1. Principle 1 – Transparency

Principle: Each member company shall provide transparency into its processing of personal data.

Guidance and Best Practices:

a. Existing NAI Guidance and/or Best Practices: N/A

b. Potential future NAI Guidance and/or Best Practices:

i. Privacy Policy Checklist - The NAI may develop a checklist & guidance about the types of information to assess for in Privacy Notices that tracks legal requirements (e.g. information about company personal data collection practices, types of personal data collected, uses, technologies, retention, sharing/disclosure, etc.).

ii. Guidance on Notice Generally - The NAI may develop resources explaining requirements for different types of notices recognized by state law and required contents of those notices – e.g. privacy notice, notice at collection, just-in-time, health-specific, etc.

iii. The NAI may develop best practices on describing digital advertising technologies to consumers.

Tools & Standards:

a. Existing Tools & Standards:

i. NAI Annual Privacy Consultation to review for presence of a Privacy Notice and for providing non-binding considerations, best practices, and surveys on the substance of such notice.

b. Potential future Tools & Standards:

i. Survey studies based on Privacy Notices provided by members.

ii. Non-binding template/model notices.

2. Principle 2 - Choice and Consumer Control

Principle: Each member company shall offer consumers method(s) to signal a choice about how the company processes their personal data, for those activities which require choice under applicable laws.

Guidance and Best Practices:

a. Existing guidance and best practices:

i. Best Practices for User Choice and Transparency

ii. Best Practices: Non-Marketing Uses of Data

b. Potential future guidance and best practices:

i. Signal Passing Provisions (e.g., how to vet & verify signals)

ii. GPC Guidance – this could cover just policy/UI implementation, or could also include technical elements like meta-data indicating what implementation of GPC is used.

Tools & Standards:

a. Existing tools and standards:
   i. NAI Opt-out pages
b. Potential future tools and standards:
   i. NAI-developed GPC extension

3. Principle 3 - Data Governance

Principle: Each member company shall take steps to ensure that its processing of personal data comports with its commitments and legal obligations.

Guidance and Best Practices:

a. Existing Guidance and Best Practices: N/A
b. Potential future guidance and best practices
   i. Contracting Guidance/Checklist
   ii. Vendor Due Diligence Guidance
   iii. DPIA checklist and best practices
   iv. Personal Data Minimization best practices
   v. Interoperability best practices
      - Potential guidance for open standard methods for technical interoperability, defined as the business-initiated "high-quality, continuous, real-time exchange of information," which is fundamental to decentralized competition and choice as well as organizational measures to distinguish personal data and non-personal data used in their interoperable exchanges with other organizations.

Tools & Standards:

a. Existing tools and standards:
   i. NAI State Law Processing Addendum
   ii. NAI Privacy Consultation Questionnaire
   iii. NAI Best Practices: Non-Marketing Uses of Data
b. Potential future tools and standards:
   i. Model DPIAs for:
      1. Targeted advertising
      2. Precise location
      3. De-identified & pseudonymous data use
   ii. De-identification approaches for Common Match Keys
   iii. Open Web Real-time Transport standards (e.g., HTTP)
   iv. Open Web Real-time Storage standards (e.g., cookie files for browsers)

4. Principle 4 - Sensitive Personal Information

Principle: Each member company shall limit its processing of sensitive personal data to disclosed purposes, and purposes consented to by the consumer as required by applicable law, and shall provide additional safeguards when processing such data.

Guidance and Best Practices:

The NAI has, and will continue to create best practices and/or guidance to help companies minimize their use of sensitive personal data, obtain consent for the use of sensitive personal information, and develop best practices for the use of inferences in areas where existing law is silent or unclear, including:

a. Existing Guidance and Best Practices:
   i. NAI Legal & Regulatory Analysis: Sensitive Health Advertising
   ii. Demographic Health Advertising Best Practices
   iii. Best Practices for User Choice and Transparency
   iv. Best Practices: Non-Marketing Uses of Data

b. Potential future guidance and best practices:
   i. NAI Precise Location Data Best Practices *(forthcoming)*

Tools & Standards (TBD):

a. Existing Tools and standards:
   i. Precise Location Information Solution Provider Voluntary Enhanced Standards

5. Principle 5 – Accountability

Principle: Each NAI member company shall demonstrate its alignment with its commitments and legal obligations tied to its processing of personal data.

Guidance and Best Practices:

a. Existing Guidance/Best Practices: N/A

b. Potential Future Guidance/Best practices:
   i. Contracting Guidance/Checklist
   ii. Vendor Due Diligence Guidance

Tools & Standards:

a. Existing tools/standards:
   i. NAI State Law Processing Addendum
   ii. NAI Privacy Consultation Questionnaire and review process
   iii. MSPA Accountability Program