Draft NAI Guidelines for Deterministic Shared Addressability Identifiers

Introduction

Since its inception twenty years ago, the NAI has sought to promote stringent standards in consumer privacy and data protection in Digital Advertising. The NAI is committed to ensuring that innovations and developments in advertising technology are matched with a set of guiding standards that ensure greater data privacy for consumers. The diverse and shifting legal landscape of today presents companies with many compliance challenges, but the NAI believes there are common policy objectives across these disparate jurisdictional legal requirements. The NAI intends to assist participants in complying with these broad policy goals by implementing fundamental standards that focus on transparency, control, data use limitations, and robust oversight and accountability.

The movement in the marketplace away from legacy pseudonymous identifiers has brought about a significant shift in the digital media ecosystem, and presents the opportunity for publishers and advertisers to play a more direct role in engaging their customers about the collection and use of data for advertising and marketing purposes. This is a positive development that holds promise for long-standing NAI priorities, including the NAI's foundational goals of enhancing consumer transparency, control, and trust in the marketplace.

To help the industry navigate this process, the NAI has developed this draft set of Guidelines for Deterministic Addressability (Guidelines). The goal of these Guidelines is to provide enforceable obligations for Participants using Deterministic Shared Addressability Identifiers (DSAIs) that will protect consumer privacy by providing transparency and control while strongly incentivizing the separation of cross-site browsing information from direct identifiers and curtailing the collection of cross-site browsing information and app use over time.

DSAIs are created by converting directly identifying information, such as an email address or phone number, into a pseudonymous, indirect identifier that may only be used to target digital advertising and measure its effectiveness. The NAI believes that the use of DSAIs must be implemented in a way to ensure that data collected across sites and apps is not linked directly to identifiable individuals, in addition to heightened limitations on the retention and use of this data across the digital media ecosystem, ensuring that these limitations and controls remain in place by all entities who wish to use these identifiers.

These Guidelines address the use of DSAIs only and do not address the use of probabilistic shared addressability identifiers, which rely on different methodologies of differentiating between devices and present a different set of privacy concerns, shifting the focus from preventing re-identification and extended retention of data, to transparency and effective consumer control.

These Guidelines are separate from the NAI Code of Conduct, and apply to website and application publishers, advertisers and agencies, ad-tech companies, data aggregators, and any other entity leveraging Deterministic Shared Addressability Identifiers. Entities utilizing DSAIs will agree to comply with the Guidelines as a condition of accessing DSAI ecosystems. NAI member companies will continue to be subject to the NAI Code of Conduct, in addition to these Guidelines where applicable based on their use of DSAIs.

The Guidelines rely on a revised NAI framework for Personal Information, but due to its narrow scope, this document only incorporates and addresses some of this terminology. This approach distinguishes between different types of Personal Information because although all these IDs are clearly "personal," they do not present the same privacy and security concerns if adopted in accordance with the technology and administrative controls established by these Guidelines.

This is a draft document, and the NAI is actively seeking input from the public. A public 60 day public comment period will begin on April 1, 2022 and end on May 30, 2022. Comments may be submitted via email to compliance@thenai.org. For those advertising industry parties interested in working in more detail with the NAI, its Board, and Members as the draft evolves based on feedback we invite you to join our Data Governance Working Group and its Addressability Subcommittee as a formal participant. Please contact membership@thenai.org for details on how to join as a participant.

In these draft Guidelines the NAI proposes how to address some of the most significant challenges posed by DSAIs and the NAI is specifically seeking feedback on the stated approach for the following key questions:

1. Consumer control:
    a. Opt-in / opt-out choices: how can the NAI achieve the appropriate level of consumer control, including where affirmative consent should be required, or where enhanced transparency and opt-out should suffice?
    b. Is there a need to preserve functionality such as measurement and attribution using DSAIs for consumers who do not consent to Tailored Advertising using a DSAI?
    c. How can the NAI ensure an effective centralized control portal for consumers across various DSAI ecosystems to ensure it can maintain and improve the NAI's industry standard of centralized choice for consumers?
    d. How can the NAI effectively distinguish the difference between retargeting in cases where an advertiser merely shows an ad and provides for measurement on a publisher's platform, as opposed to collection and combination of a consumer's data across different websites, apps, or businesses they directly interact with?

2. Linkage to directly identifiable data:

   The NAI has observed email addresses as the predominant basis for DSAIs. However advertisers and other businesses may utilize telephone numbers as well, and potentially street addresses, which may be more easily re-identified to a known individual. What types of additional controls can be provided to ensure that use of telephone numbers or postal addresses are not re-identified to specific individuals?

3. Sensitive Information

   Is it possible to reconcile the use of DSAIs in measurement subsequent to contextual or other non-Tailored Advertising, where the context of the application or website communicates Sensitive Information, such as an app focused on the LGBTQ+ community, a medical condition, or a specific ethnic group?

4. Accountability and enforcement:

   What additional technical and administrative controls could the NAI consider to ensure the highest level of auditability and accountability across various Participants?

I. Definitions

A. Consumer Choice Mechanism:

A Consumer Choice Mechanism is a clear, conspicuous, and easy to use mechanism through which consumers may express their consent preferences for data collection and use for Tailored Advertising.

B. Deterministic Shared Addressability Identifier (DSAI)

A Deterministic Shared Addressability Identifier (DSAI) is a unique identifier that is created by converting a Direct Identifier so that it cannot reasonably be used to directly identify a consumer but allows multiple parties to pseudonymously distinguish the same consumer over time and across websites, applications, and devices. DSAIs include hashed email addresses, hashed telephone numbers, and hashed postal addresses. Deterministic Shared Addressability Identifiers do not include encrypted versions of such identifiers that can only be decrypted by the Participant or other Participants, where the encryption changes frequently enough to reasonably prevent the collection of Usage Information over time in combination with the DSAI (no more than every 24 hours).

Commentary: Encrypted forms of a hashed email address cannot be used to understand the underlying information and cannot be used to target advertising based on data associated with the hashed email address. So long as the encryption changes frequently enough, allowing for the encrypted version of the identifier to change at least daily, this helps ensure that it does not provide a stable identifier that can be used to collect Usage Information over time. Consequently, those companies that receive or transfer only encrypted versions of DSAIs are not subject to these Guidelines.

C. Participant

A Participant is an entity that agrees to be bound by these Guidelines and uses a Deterministic Shared Addressability Solution to create or access DSAIs.

D. Direct Identifier – Direct Identifiers are identifiers that allow the direct identification of consumers and include name, address, telephone number, email address, financial account numbers, and government-issued identifiers.

E. Usage Information – Usage Information is information, about a consumer, browser, or device's activity on, or interaction with, a website, application, or other digital content, including audio and connected television programming, not owned by the Participant, including any inferences based on that activity or interaction. Usage Information does not include any information that a Participant collects in a first-party context, including any information a Participant collects directly from consumers, information about

consumers' engagement with a Participant's own properties, or information about a consumer's purchases made with the Participant.

F. Marketing Information – Marketing Information is information about a consumer, including transactions, inquiries, preferences, demographic characteristics, survey responses, or market research, including any inferences based on that information. Marketing Information does not include any information that a Participant collects in a first-party context, including any information a Participant collects directly from consumers, information about consumers' engagement with a Participant's own properties, or information about a consumer's purchases made with the Participant.

G. Service Provider

A Service Provider is an entity that processes Direct Identifiers, DSAIs, Usage Information, or Marketing Information on behalf of a Participant pursuant to a contract that prohibits the entity from retaining, using, or disclosing the information for any purpose other than to perform the services specified in the contract. Participants who decrypt DSAIs and make them available to other Participants for Tailored Advertising purposes are not acting as Service Providers.

H. Tailored Advertising

Tailored Advertising is:

1. Selecting an advertisement to display to a consumer that is based on Usage Information;
2. Selecting an advertisement to display to a consumer on websites, mobile applications, or other online services not owned or operated by the Participant that is based on Marketing Information;
3. Tailored Advertising does *not* include:
    a. Advertising to a consumer in response to a request for information or feedback;
    b. Advertisements based on activities within a Participant's own websites or online applications, or transactions with the Participant; and
    c. Advertisements based on the context of a consumer's current search query, or current interaction with a website, application, or other digital content such as current audio or current video programming.

I. Opt-In Consent

Opt-In Consent is an affirmative action taken by a consumer that manifests the intent to opt in to an activity described in clear and conspicuous notice. Opt-In Consent must be revocable.

J. All other definitions can be found in the 2020 NAI Code of Conduct.

II. General Requirements

A. These Guidelines are not intended to address or restrict any disclosure, transfer, or sharing of information, including DSAIs, Direct Identifiers, Usage Information, and Marketing Information with Service Providers.

B. All Participants must comply with all applicable laws, regulations, and existing self-regulatory principles, in the United States, including existing Principles promulgated by the Digital Advertising Alliance (DAA) at the time of publication of these Guidelines.

C. Participants shall not use Social Security Numbers, other non-public government-issued identifiers, financial account numbers, or other similarly sensitive Direct Identifiers to create a DSAI.

D. Participants shall only use, or permit the use of, a DSAI for advertising and marketing purposes, including ad targeting, selection, segmentation, modeling, measurement, and attribution.

E. Participants shall not use, or permit the use of, a DSAI to make any eligibility determinations about consumers, including for health care, insurance, employment, credit, tenancy or housing, or education.

III. Data Provenance

These are requirements for Participants creating or licensing a DSAI for any permitted purpose.

A. Participants shall only create a DSAI using Direct Identifiers collected directly from the consumer to whom the DSAI relates.

B. In order to create a DSAI, Participants shall provide clear and conspicuous notice informing consumers that:
   1. The consumers' email addresses, telephone numbers, or other permitted Direct Identifiers will be used for advertising purposes;
   2. The Direct Identifiers will be hashed before being shared with partners for the purposes of delivering relevant advertising and/or measurement of advertising's effectiveness; and
   3. The consumers may, at any time withdraw consent for the Participant's use of the DSAI for Tailored Advertising purposes, along with instructions for such withdrawal of consent, if the Participant uses DSAI's for Tailored Advertising.

C. Participants may license DSAIs from other parties only if:

1. The Participant is able to identify the party that initially collected the Direct Identifier used to create the DSAI; and
2. The party that initially collected the Direct Identifier used to create the DSAI did so in accordance with the requirements present in section III.A-B above, as well as all applicable laws, regulations, and existing self-regulatory principles in the United States, including existing Principles promulgated by the Digital Advertising Alliance (DAA) at the time of publication of these Guidelines.

IV. Notice

A. *Direct Notice:* When creating or using a DSAI, Participants shall disclose the following in their privacy policies:
   1. A description of how the Participant creates, collects, uses, and discloses DSAIs and that this process is based on converting a consumer's Direct Identifier so that it is no longer directly identifiable.
   2. That the DSAI may be shared with other Participants who may also hold Direct Identifiers relating to the consumer, and used by the Participant and other Participants to facilitate Tailored Advertising as well as to measure the effectiveness of advertising;
   3. That consumers may, at any time, revoke consent for the use of the DSAI for Tailored Advertising by the Participant, with a link to, and/or instructions for, the Participant's Consumer Choice Mechanism for Tailored Advertising.
   4. Participants creating or using multiple DSAIs for Tailored Advertising, created from the same Direct Identifier, shall disclose each DSAI ecosystem the Participant engages in, as well as a link to additional information about each DSAI ecosystem.

   Commentary: There are multiple ID mechanisms available for digital advertising use. Section IV.A.4. requires Participants using more than one of these shared ID mechanisms to disclose each mechanism.

V. Consumer Control for use of DSAIs for Tailored Advertising

These are requirements for Participants using a DSAI for Tailored Advertising.

A. Participants shall only use a DSAI for Tailored Advertising purposes with the Opt-In Consent of the consumer to whom the DSAI relates.

B. Participants shall provide a Consumer Choice Mechanism that enables consumers to revoke their consent for the Participant's Tailored Advertising with the consumers' DSAI.

C. Participants shall only use a DSAI for Tailored Advertising purposes that provides, or is integrated with, a central Consumer Choice Mechanism that enables consumers to revoke their consent for the use of their DSAI for Tailored Advertising.

VI. Susceptible Information

A. Participants collecting, disclosing, or otherwise sharing the following types of information in combination with a DSAI shall obtain the consumer's Opt-In Consent:

1. Sensitive Information;

2. Sensor Information;

3. Personal Directory Information;

4. Precise Location Information;

5. Information, including inferences, about a consumer's engagement with or interest in explicit sexual content or material; and

6. Information, including inferences, about a consumer's sexual orientation, racial or ethnic origin, religious beliefs, union membership, citizenship, or immigration status, unless such information is publicly available;

Commentary: Participants engaging in collecting, disclosing, or otherwise sharing Susceptible Information in combination with a DSAI must obtain a consumer's Opt-In Consent specific to the type(s) of Susceptible Information and use cases in question, distinct from general Opt-In Consent for the use of a DSAI for Tailored Advertising.

B. Participants may not create a DSAI for consumers they know to be under 16 years old, or otherwise use a DSAI to knowingly engage in Tailored Advertising to consumers under 16.

VII. Data Stewardship

A. Participants shall employ reasonable technical, administrative, and procedural safeguards to protect the security of DSAIs and any information associated with DSAIs, including Usage Information.

B. In order to protect the integrity and security of DSAI ecosystems, Participants shall only disclose DSAIs to other Participants of the same DSAI ecosystem.

C. Participants shall retain any Usage Information collected with a DSAI only so long as necessary for the purpose for which it was collected, and no longer than 13 months.

D. Participants shall not link, or cause to be linked, Usage Information with Direct Identifiers, except and solely to the extent necessary to comply with a specific obligation of an applicable law.

E. Participants that access Usage Information collected with a DSAI, and Direct Identifiers, shall put in place technical and procedural controls to prevent the re-identification of said Usage Information.

VIII. Accountability and Enforcement

A. Participants shall undergo an initial review by the NAI, or its designees, to determine that the Participant is in a position to comply with these Guidelines. Participants shall undergo annual reviews of their compliance with these Guidelines, by the NAI or its designees, and shall undertake any required remediation measures resulting from such reviews as detailed in [external Security/Compliance/Enforcement Procedures annex].

B. Participants that access Usage Information collected with a DSAI, and Direct Identifiers, shall be subject to additional security terms and obligations, including demonstration of compliance with these Guidelines through additional security audits by the NAI, or its designees, on an annual basis as described in [external Security/Compliance/Enforcement Procedures annex].

C. If Participants' access to Shared Addressability Solutions is conditional on their compliance with these Guidelines, such access may be restricted or terminated when the Participants violate or otherwise fail to comply with these Guidelines, subject to [external Security/Compliance/Enforcement Procedures annex].

Under the revised NAI approach to data and identifiers, *all* the identifiers and information below are considered Personal Information.

Identifiers
Indirect Device Identifier Indirect Device Identifiers are unique identifiers associated with browsers or devices which may be used to Indirectly distinguish separate browsers or devices. Indirect Device Identifiers include unique cookie identifiers, unique mobile advertising identifiers, and IP addresses, so long as that information does not directly identify a consumer, or the activity of a consumer across multiple devices.
Indirect Consumer Identifier Indirect Consumer Identifiers are unique identifiers associated with consumers which may be used to Indirectly distinguish consumers on a browser or device, or across multiple browsers or devices. Indirect Consumer Identifiers include hashed email addresses, hashed postal addresses, hashed telephone numbers, or Deterministic Shared Addressability Identifiers, that cannot reasonably be used to directly identify a consumer. *Indirect Consumer Identifiers do not include encrypted versions of such identifiers, or tokens, if such encryption reasonably prevents the collection of Usage Information over time in combination with the Indirect Consumer Identifier.*
Direct Identifier Direct Identifiers allow the direct identification of consumers, and include name, address, telephone number, email address, financial account numbers, and government-issued identifiers.

Information
Usage Information Usage Information is information, about a consumer, browser, or device's activity on, or interaction with, a website, application, or other digital content such as audio and connected television programming, not owned by the Participant, including any inferences based on that activity or interaction. Usage Information does not include any information that a Participant collects in a first-party context, including any information a Participant collects directly from consumers, information about consumers' engagement with a Participant's own properties, or information about a consumer's purchases made with the Participant.
Marketing Information Marketing Information is information about a consumer, including transactions, inquiries, preferences, demographic characteristics, survey responses, or market research, including any inferences based on that information. Marketing Information does not include any information that a Participant collects in a first-party context, including any information a Participant collects directly from consumers, information about consumers' engagement with a Participant's own properties, or information about a consumer's purchases made with the Participant