The NAI Mobile Application Code:
Extending Third-Party Compliance into the Mobile Ecosystem
Why a Mobile Application Code?

• Extend the NAI compliance program into the mobile application space
• Provide extra flexibility for this rapidly developing ecosystem
• Help members develop business models, procedures, and technologies that provide consumers with adequate notice and choice
Scope

• Governs only NAI member companies

• Does not cover all data collection by members, but is limited to Cross-App Advertising and Ad Delivery and Reporting

• Advertising data collected across unaffiliated websites in mobile browsers will be covered by the 2013 NAI Code of Conduct, with mobile-specific guidance as necessary

• Applies only to activities that (1) occur in the United States or (2) apply to U.S. users
Member Obligations

- Education
- Notice & Transparency
- Choice/User Control
- Use Limitations
- Transfer Restrictions
- Access
- Reliable Sources
- Data Security & Retention
- Accountability
General Framework

- The Code identifies three broad categories of data:
  1. Personally Identifiable Information (PII)
  2. Non-PII
  3. De-Identified Data

- The Code also imposes special obligations on:
  1. Sensitive Data
  2. Precise Location Data; and
  3. Personal Directory Data
Three Types of Notice

Website Notice:

• Describes data collection, use, and transfer for CAA & ADR

• Describes or provides access to an opt-out mechanism
Three Types of Notice

App Store Notice:

• Posted in any store or on any website where the app may be acquired

• Must be included in contractual agreements with individual app providers, if such contracts exist
Three Types of Notice

Enhanced Notice:

- Notice in or around ads informed by Cross-App Data
  or
- In the app settings and at download or first use.
Health Transparency

• Members that use standard interest segments based on health-related data must disclose those segments on their websites.

• Health-related data is anything related to the body, including:
  • Health & wellness;
  • Diet & fitness;
  • Migraines
  • Etc.
User Control for Cross-App Advertising

- Use of Non-PII for CAA requires access to an Opt-Out Mechanism.
- Prospective merger requires access to an Opt-Out Mechanism and robust notice.
- Retrospective merger and use of Sensitive or Precise Location Data requires Opt-In Consent.
- May not access a device to obtain Personal Directory Data without user authorization.
Opt-Out Mechanism

- No industry-wide mechanism (yet)
- Code requires that any Opt-Out Mechanism be: (1) reasonably easy to use and (2) durable.
- Platform-provided tools (like iOS’s Limit Ad Tracking feature) may meet this requirement.
- Individual member mechanisms will be evaluated during pre-certification.
Use Limitations

- Members may not create Cross-App Advertising segments targeting children under 13 without obtaining verifiable parental consent.
- Members may not use or allow the use of Cross-App or ADR data for:
  1. Employment Eligibility
  2. Credit Eligibility
  3. Health Care Eligibility
  4. Insurance Eligibility and Underwriting and Pricing
- Material changes require Opt-In Consent
Transfer Restrictions

• When transferring PII to an unaffiliated party for Cross-App Advertising or Ad Delivery & Reporting, must contractually require that the unaffiliated party will adhere to the applicable provisions of the code.

• When transferring Non-PII collected across applications, the unaffiliated entity must not attempt to merge that Non-PII with PII or attempt to re-identify the individual. This does not apply if the Non-PII is proprietary to the receiving party.
Data Access, Quality, Security & Retention

Members must:

• Provide reasonable access to PII;

• Conduct due diligence to ensure the obtain Cross-App Data from reliable sources (notice & choice);

• Provide reasonable security for ad data; and

• Only hold data as long as necessary to fulfill a legitimate business need, or as required by law.
Accountability

• Members must represent that their business practices are in compliance with the NAI Mobile Application Code.

• Members are required to undergo annual compliance reviews. The aggregate results of the annual compliance process are published.

• Members must provide a mechanism to receive consumer complaints and inquiries and make reasonable efforts to timely respond to concerns regarding compliance with the NAI Code.
DIFFERENCES BETWEEN THE NAI & DAA MOBILE CODES
Difference between DAA & NAI Codes

• NAI always requires notice on member website.

• NAI notice requires:
  • A general description of the technologies used for data collection;
  • Data retention practices/limits; or
  • Standard interest segments based on health-related information.

• NAI requires app store notice.

• NAI distinguishes between PII and Non-PII.
Q&A