# 2015 ANNUAL COMPLIANCE REPORT

NAI
Network Advertising Initiative

# A LETTER FROM NAI VICE PRESIDENT FOR COMPLIANCE AND POLICY

**ON BEHALF OF THE NETWORK ADVERTISING INITIATIVE (NAI) AND OUR COMPLIANCE TEAM, I AM PROUD TO PRESENT THE NAI 2015 ANNUAL COMPLIANCE REPORT.** The Report provides a summary of members' adherence to the NAI Code of Conduct (Code) based on findings from the NAI staff's ongoing monitoring processes during the 2015 compliance period (January 1 to December 31, 2015).

Not only is the Code, most recently updated in 2015, one of the highest standards for self-regulation in the ad-tech industry, but the Code is also backed by rigorous compliance procedures. The compliance process is a priority for us because we know that even the highest standards for self-regulation are meaningless without an insistence on accountability.

While the Compliance Report comes out once a year, the compliance process is year-round and includes both manual and automated monitoring of opt-outs and changes to privacy disclosures. The conclusion of this year's Report is that members are overwhelmingly meeting the requirements of the Code. When our compliance staff found some nonmaterial issues, we were able to work with members to rectify them in a prompt manner. Publishing this Report allows consumers, members, regulators and other interested parties to evaluate the compliance program and self-regulatory process for themselves.

One important takeaway from the 2015 compliance process is the strong commitment members consistently show to NAI's high standards for data collection and use. Our members frequently sought guidance from NAI staff in one-on-one conversations to ensure that they are correctly applying the Code to their business practices. NAI staff held face-to-face meetings with members in order to learn more about their business models and technologies and to answer questions from their internal compliance teams. We know that members value these interactions because, in 2015, they regularly sought assistance in applying our principles to new, emerging technologies and business lines.

Not only does constant communication with members help to proactively mitigate compliance problems, it also results in an even more knowledgeable and strong NAI compliance team. It is the NAI staff's technical understanding of the industry that gives us the ability to provide members with meaningful guidance. Every year, questions around privacy hinge on more complex and nuanced technical issues. We believe that the staff's knowledge base will be crucial in the upcoming year as members begin to look into new technologies and sources for data collection that are intricate and varied. Open, collaborative discussions with NAI compliance staff demonstrate members' commitment to protecting consumer privacy while building thriving online businesses.

Without question, NAI's effective self-regulation program is the best strategy for responding to the challenges around changing business practices, technological advances, and consumer expectations in an industry where innovation comes at an exceptionally rapid pace. Specifically, the ad tech industry is continually evolving toward a future where unique challenges may arise in providing effective notice and choice to consumers. However, NAI members are consistently adjusting and creating groundbreaking new tools to provide consumers with more transparency around their data collection and use practices.

We know that our industry is at a turning point. But our compliance staff and member companies continue to prove their ability and willingness to fine tune self-regulatory frameworks to address new and challenging issues. Members' careful application of our principles, overseen by a sophisticated compliance staff, will help steer our industry through increasingly complex issues for years to come.

**Noga Rosenthal**
General Counsel, VP for Compliance and Policy

# EXECUTIVE SUMMARY

The Network Advertising Initiative (NAI) is a leading non-profit self-regulatory association governing technology companies engaged in digital advertising. It is a membership organization, comprised of approximately 100 third-party digital advertising companies. The vast majority of Internet ads served in the United States involve the technology of one or more of the NAI's member companies. NAI members provide the infrastructure for the tailored advertising that enables a thriving and diverse ecosystem of ad-supported content and services. The NAI's role is to help promote consumer privacy and trust in this ecosystem by creating and enforcing high standards for responsible data collection and use practices among its member companies. The NAI accomplishes this goal through a body of self-regulatory policies accompanied by a robust compliance and enforcement program that helps member companies meet the NAI's high standards.

## NAI CODES OF CONDUCT

The NAI first developed and adopted a set of self-regulatory policies for online advertising, based on the Fair Information Practice Principles (FIPPs), in 2000. Since then the NAI has updated its Code of Conduct (Code) three times, most recently in 2015, to keep pace with evolving technology and member company business models. The Code not only requires member companies to provide notice and choice with respect to Interest-Based Advertising (IBA), but also imposes a host of substantive restrictions on member companies' collection, use, and transfer of data for IBA. All members engaged in IBA are required to comply with the Code.

In addition to the Code, which covers members' IBA activities across unaffiliated websites, the NAI first released its Mobile Application Code (App Code) in 2013 to cover members' advertising-related data collection and use across mobile applications. The App Code applies the same Code principles, based on the FIPPs, in a mobile environment. Member compliance with the App Code was previously voluntary as the mobile advertising ecosystem matured, but it became mandatory as of January 1, 2016 for all members engaged in Cross-App Advertising (CAA).

> "NAI compliance is an essential credential for our business. The NAI's compliance process provides us with an outside perspective on what we do and helps us ensure that we are incorporating consumer privacy into our products from inception."
>
> Alex Gove, VP Corporate Development, RadiumOne

"NAI staff is always accessible to offer guidance. As technology changes, they discuss issues and answer questions to help companies compete and keep privacy a priority."

Stephanie King, General Counsel, AdRoll

## 2015 UPDATES AND GUIDANCE

In 2015 the NAI published updates to both the Code, and the App Code. These updates clarified a number of interpretations of existing obligations. The NAI also released two key pieces of additional guidance for its members:

*Guidance for NAI Members—Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI Code of Conduct*: This guidance addresses member use of evolving technologies and clarifies how members may use non-cookie technologies for IBA in a manner consistent with the Code. As part of this process the NAI designed a new industry opt-out page enabling consumers to review whether an NAI member company is customizing their advertising experience regardless of the technology used, and to enable consumers to exercise choice when new technologies are used.

*Guidance for NAI Members—Determining Whether Location is Imprecise:* This guidance gives members more direction when evaluating the relative precision of location data and provides a number of best practices in rendering location data imprecise.

In the area of cross-device association and targeting, the NAI's policy work included staff representation on both panels at the U.S. Federal Trade Commission (FTC) Workshop on Cross-Device Tracking and input by NAI members and staff in the drafting of the Digital Advertising Alliance (DAA) Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices.

# COMPLIANCE OVERVIEW

In an effort to provide a highly effective self-regulatory framework for the third party advertising technology industry, that engenders the trust of all stakeholders, the Code is backed by a rigorous compliance process, and the availability of strong enforcement methods when necessary. The NAI conducts year-round compliance activities that include:

**Pre-Membership Review:**
NAI staff and the NAI Board of Directors evaluate prospective members' business models, technologies, consumer choice mechanisms, public disclosures, and partner contract provisions to help confirm that they are able to meet the requirements of the Code, and the commitments they make in their own privacy disclosures.

**Technical Monitoring:**
The NAI conducts automated technical monitoring of members' opt outs and changes to privacy disclosures to help ensure members' compliance with the Code.

**Investigation of Consumer Communications:**
The NAI investigates consumer allegations that a member may not be complying with the Code and works with members to address potential violations.

**Investigation of Allegations of Non-Compliance:**
The NAI evaluates allegations of non-compliance with the Code from other sources, such as regulators, competitors and privacy advocates.

**Annual Compliance Reviews:**
The NAI performs in-depth, annual reviews of members to help them ensure that their business operations are able to continue to comply with the Code and their own privacy disclosures—even as their business models evolve.

**Enforcement:**
NAI members are subject to formal sanctions for material non-compliance with the Code or their own privacy disclosures.

**Publication of the Annual Compliance Report:**
The NAI provides consumers, regulators and others visibility into the NAI's compliance program and self-regulatory process through the publication of this annual compliance report.

## Through the 2015 compliance review process, NAI found that member companies are overwhelmingly meeting the requirements of the 2015 Update to the NAI Code of Conduct.

| | |
|---|---|
| **Education (§ II.A.)** | In 2015, members estimated that they donated billions of impressions to the NAI's education campaign. This campaign worked to educate consumers about IBA and available choice mechanisms, leading to over 5.3 million page views of the NAI consumer education pages in 2015—nearly 20% more visits than in 2014. |
| **Transparency and Notice (§ II.B.)** | Members continued to provide consumer-facing notice of their data collection and use practices for IBA and Ad Delivery and Reporting (ADR).<br>1. First, members provided notice in their privacy disclosures on their own sites regarding their IBA and ADR activities.<br>2. Second, members worked to ensure that the digital properties or publishers with which they partner for IBA activities post notice and choice around these activities on their consumer-facing sites.<br>Member companies also provided notice and choice in or around advertisements through an enhanced notice mechanism.<br>Members worked to disclose the standard health segments they used for IBA. |
| **User Control (§ II.C.)** | All NAI members offered links to Opt-Out Mechanisms from their own sites. There were more than 7.5 million visits to the NAI opt-out page in 2015—over two million more visits than reported in 2014.<br>The NAI's Opt-Out Scanner and NAI staff's manual checks of members' Opt-Out Mechanisms revealed that members provided and honored consumer choice with respect to the collection and use of data for IBA. |
| **Use Limitations (§ II.D.)** | Members expressly affirmed their compliance with Code limitations around the use of data collected for IBA and ADR purposes, confirming that the data was not used, or allowed to be used, for eligibility purposes, such as health insurance eligibility. |
| **Transfer Restrictions (§ II.E.)** | Members attested to their compliance with Code requirements limiting the transfer of data collected for IBA and ADR purposes to third parties, limiting the recipient's ability to re-identify individuals for IBA purposes without Opt-In Consent where Non-PII is not proprietary to the receiving party. |
| **Data Access, Quality, Security & Retention (§ II.F.)** | Members confirmed during the annual review that they retained the Non-PII data collected for IBA purposes in accordance with their publicly posted retention periods and attested to reasonable security for their systems and data. |

## 2015 ANNUAL COMPLIANCE REVIEW

NAI staff found that evaluated member companies were materially in compliance with the Code, and also found that members took proactive steps to ensure that they remained in compliance with the Code throughout the year.

Partly as a result of the NAI's increased monitoring capabilities, NAI staff found a number of nonmaterial issues throughout the compliance period. In all such cases NAI staff worked with members to rectify any issues promptly, before these potential infractions could turn into larger problems affecting greater numbers of consumers. For example, NAI staff discovered that several members' email links for consumer questions did not appear to function as intended. The NAI notified all such members and each company indicated that it was working to fix the issue once the matter was brought to its attention.

Throughout 2015 the NAI also maintained its longstanding policy of reserving strong sanctions procedures for willful or material violations of the Code, while working with member companies to resolve minor, non-material violations of the Code as quickly as possible. During the year, NAI staff conducted several investigations regarding potential material non-compliance with the Code and when appropriate, NAI staff consulted the NAI Board of Directors Compliance Committee. In all such cases reviewed between January 1, 2015 and December 31, 2015, the NAI either did not find a violation of the Code or found that the alleged activities were not, at the time, covered by the NAI's enforcement efforts on mobile devices.

## LOOKING FORWARD

As this Compliance Report looks back on 2015, the NAI is laying the groundwork for its plans in 2016. The NAI plans to further improve its consumer education materials, including more information on new technologies and data collection across mobile applications. 2016 is the first year that all evaluated member companies engaged in cross-app data collection and use for advertising purposes will be required to undergo a full compliance review of such activities. The results of that review will be made available in the 2016 Annual Compliance Report. The NAI also plans to begin work on synthesizing its Code and App Code into one document in order to make NAI requirements easier to grasp for the public, and to streamline compliance efforts for NAI members. The NAI will also continue to work with its members and with industry stakeholders as it further explores a role for potential guidance regarding Cross-Device applications in online advertising.

On the technical front, the NAI is pursuing further enhanced monitoring capabilities, focused on data collection across mobile applications and other cookie-less technologies. These developments will coincide with the planned public launch of the revamped NAI opt-out page, enabling consumers to verify when NAI members are collecting and using data for IBA with non-cookie technologies, and facilitating consumer choice when non-cookie technologies are used for IBA.

As NAI members continue to encounter challenges in applying responsible privacy practices to emerging technologies and business lines, the NAI is able to leverage its unique position in the advertising technology ecosystem to maintain a pulse on what companies are doing, and where to next focus its resources in years to come.

# INTRODUCTION

Since 2000, the Network Advertising Initiative (NAI) has been a leading self-regulatory body governing "third parties" engaged in Interest-Based Advertising (IBA)[1] and Ad Delivery and Reporting (ADR)[2] in the United States.[3] At the time of publication, the NAI has 101 member companies. NAI members include a wide range of businesses such as ad networks, exchanges, platforms,[4] data aggregators, and other technology providers. Across websites and mobile applications, these intermediaries form the backbone of the digital advertising ecosystem—helping advertisers reach audiences most likely to be interested in their products and services while allowing consumers to receive ads that are relevant to their interests. This relevant advertising, in turn, continues to power free content and services in the digital ecosystem, including websites and mobile applications.[5]

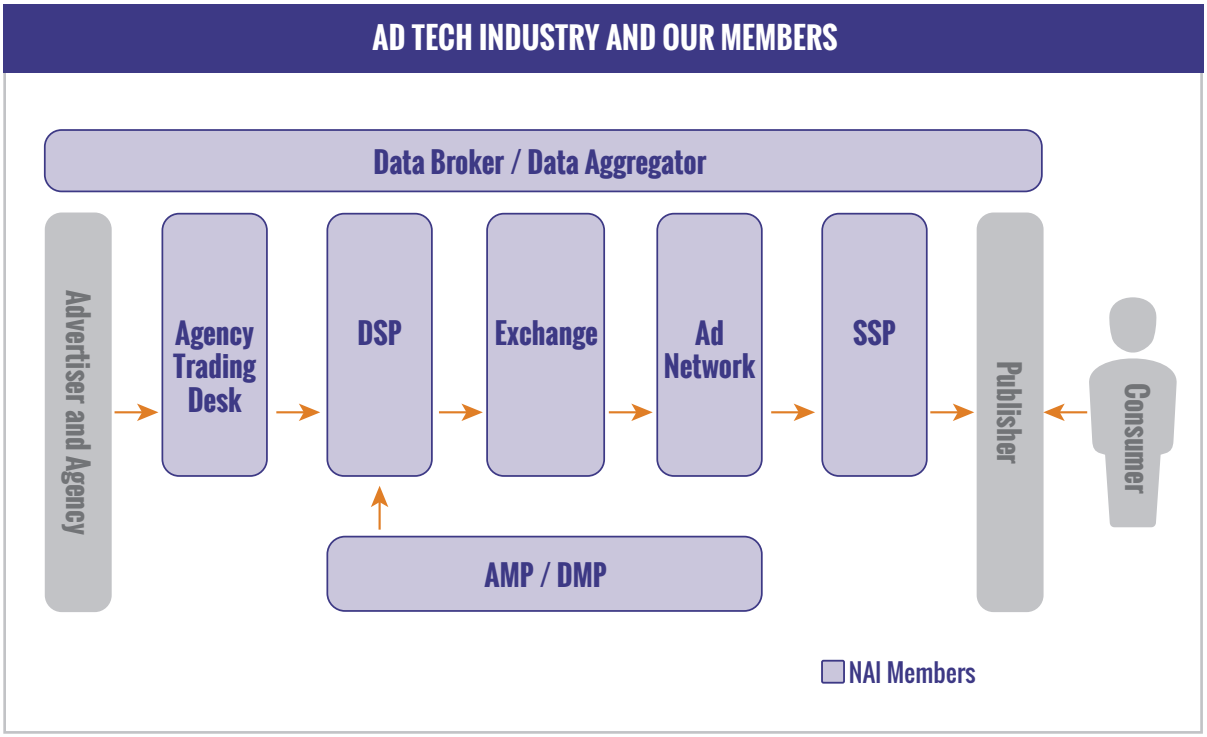
1 IBA is defined in the 2015 Update to the NAI Code of Conduct as "the collection of data across web domains owned or operated by different entities for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected" (§ I.A.).

2 The 2015 Update to the NAI Code of Conduct imposes requirements with respect to "Ad Delivery & Reporting," which are separate and distinct activities from IBA. Ad Delivery and Reporting (ADR) is defined as "the logging of page views or the collection of other information about a computer or device for the purpose of delivering ads or providing advertising-related services." ADR includes providing an advertisement based on a browser or time of day, statistical reporting, and tracking the number of ads served on a particular day to a particular website (§ I.B.).

3 The 2015 Update to the NAI Code of Conduct covers activities that occur in the United States, or affect consumers in the United States. While the NAI encourages its members to apply the high standards of the Code to their IBA and ADR activities globally, the NAI only evaluated US-based IBA, Retargeting, and ADR activity for the purposes of this compliance report.

4 NAI membership spans various technology platforms, including demand side platforms (DSPs), supply side platforms (SSPs), data management platforms (DMPs) and audience management platforms (AMPs).

5 *See* J. Howard Beales & Jeffrey A. Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, Navigant Exonomics (Jan. 2014), available at www.aboutads.info/resource/fullvalueinfostudy.pdf (offering relevant advertising to visitors benefits smaller websites providing essential revenue to the "long tail").




Member companies work together with NAI staff to help craft stringent yet practical guidelines for data collection and use in connection with IBA and ADR. Ultimately, the goal of the NAI is to maintain consumer trust by protecting consumer privacy while enabling member companies to provide a relevant digital advertising experience. The NAI helps its members foster this trust through a comprehensive self-regulatory program that includes codes of conduct backed by robust compliance, enforcement, and sanctions.

This report provides a summary of the NAI's achievements in 2015 as well as staff's findings from the 2015 compliance review. During the 2015 compliance period, NAI staff reviewed members' compliance first with the 2013 Code of Conduct (2013 Code),[6] which was in effect from the outset of the compliance period on January 1, 2015 until May 31, 2015, and subsequently the 2015 Update to the NAI Code of Conduct (Code),[7] which was enforced from June 1, 2015 until the end of the compliance period on December 31, 2015. This report is intended to provide consumers, regulators and others with visibility into the NAI's compliance program and self-regulatory process. In addition, this report helps illustrate how the compliance process shapes the evolution of the NAI's policies and procedures, including goals for further evolution of NAI policy, guidance, and compliance program in 2016, to assure that the NAI continues to offer a vibrant self-regulatory program that responds to new issues and technologies in a practical way.

6 *See 2013 NAI Self-Regulatory Code of Conduct, available at* www.networkadvertising.org/2013_Principles.pdf.

7 *See 2015 Update to the NAI Code of Conduct, available at* www.networkadvertising.org/2015NAICode.pdf.

# 2015: A YEAR IN REVIEW

The NAI's self-regulatory program continues to evolve, mature, and expand. As has become its custom, the NAI set forth its goals for the following year in its 2014 Annual Compliance Report. In the last report, the NAI committed to: (1) finalize its education page to more effectively inform consumers about IBA and Cross-App Advertising (CAA) in the mobile world; (2) release an updated version of the Code; (3) release an updated version of the Mobile Application Code (App Code); (4) release final guidelines for the use of non-cookie technologies for IBA and ADR; (5) develop a new opt-out page for members and consumers to facilitate choice as it applies to these new technologies; and (6) work to develop policies coinciding with the maturation of technologies that facilitate the linking of devices presumed to belong to the same consumer or household. The NAI achieved and, in some cases, surpassed these goals.

In many ways, 2015 was a banner year for the NAI. In March the NAI welcomed its new President and CEO, Leigh Freund. She joined the NAI from NAI Board member company AOL Inc., where she served as Vice President and Chief Counsel for Global Public Policy. Outgoing President and CEO, Marc Groman, who had spent the previous three years working tirelessly on behalf of the NAI, joined the White House Office of Management and Budget as Senior Advisor for Privacy.

In May the NAI released the most recent update to the Code. This update made several important clarifications regarding the NAI's interpretation of Code requirements, but did not add new substantive requirements for member companies. For example, the Code clarifies that the practice of Retargeting[8] by NAI members carries the same obligations as IBA, and that Retargeting is fully covered by the Code and the NAI's compliance efforts. The NAI had always intended for its requirements for IBA to apply equally to Retargeting, and for clarification this explanation was moved from the commentary to the text of the Code itself. The Code also further clarifies the definition of Sensitive Data, explaining that in addition to specific knowledge, it also includes inferences about certain health or medical conditions. The revised definition of Sensitive Data distinguishes between two types of sensitive medical information, including sensitive sources, such as medical or pharmaceutical records, and sensitive conditions, such as sexually-transmitted diseases or mental health-related conditions.

8 Retargeting is defined in the Code as "the practice of collecting data about a user's activity on one web domain for the purpose of delivering an advertisement based on that data on a different, unaffiliated web domain" (§ I.C.).

In concert with the release of the Code, the NAI also published its *Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI Code of Conduct* (Guidance on Non-Cookie Technologies). This document was the culmination of years of work by NAI members and staff in creating a framework for self-regulation of the use of emerging technologies for IBA. As part of this process, the NAI designed a new industry opt-out page for consumers, unveiled to its members at the 2015 NAI Summit. This tool was designed to inform consumers when an NAI member company customizes their advertising experience with non-cookie technologies and facilitates consumer choice when new technologies are used.

Also in May the NAI hosted its third annual Summit, returning to New York City. This event provided member companies with an opportunity to join robust discussions about the latest technologies, regulatory and legislative trends, and emerging business models. NAI members, staff, technology executives, and prominent industry experts participated in panels ranging from Cross-Device linking to the Internet of Things, and the latest developments in the European Union.

**In 2015, 13 new companies were approved for NAI membership.**

The NAI released an update to the App Code in August, to further clarify how the principles found in the Code apply in the growing mobile CAA ecosystem. This App Code update incorporated many of the changes that were introduced in the Code, as discussed earlier. It also integrated feedback the NAI received from a variety of sources since the publication of the original App Code in 2013. In 2015 evaluated member companies were able to undergo voluntary compliance reviews with the App Code, with the assistance of NAI staff. The App Code's effective enforcement date for all members began January 1, 2016. Therefore, all evaluated member companies will go through a full mandatory compliance review with the App Code in 2016.

**In 2015, the NAI website saw over 8.2 Million unique visitors, up 45% from 5.6 Million in 2014.**

Due to certain challenges posed by technological monitoring and the provision of an easy to use choice mechanism in conjunction with the small-screen experience inherent in mobile web browsers, the NAI previously limited its enforcement of the Code to member companies' data collection and use for IBA in web browsers on desktop and laptop computers. As the NAI and its members worked to overcome these challenges, the NAI was able to begin full enforcement of the Code on data collection and use for IBA in mobile web browsers in September 2015. In 2016 the NAI is fully enforcing its Code in regard to member data collection and use for IBA across websites on mobile web browsers, and its App Code in regard to member data collection and use for CAA across mobile applications.

NAI members and staff, together the with NAI Board of Directors, worked throughout the year to identify the most pressing privacy issues associated with linking devices for IBA, CAA, or ADR purposes. During this time, the NAI worked closely with staff at the Federal Trade Commission (FTC), culminating in the November 2015 FTC Workshop on Cross-Device Tracking.[9] NAI staff participated on each panel. The NAI, through its position on the Digital Advertising Alliance (DAA) Board of Directors, and its members, as participants in the DAA's self-regulatory program, also provided input to the DAA in the drafting of the *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices*.[10] This guidance is an important first step in addressing the privacy challenges presented by cross-device association. The NAI continues to explore the privacy concerns of linking devices for advertising purposes and whether additional guidance, specifically for NAI members, would be appropriate.

Demonstrating the continued need for strong self-regulation among advertising technology companies, the NAI saw a significant influx of new member applications in 2015, with 13 new companies joining the NAI after approval by the NAI Board of Directors and completion of the new applicant review process.

In addition to the increased interest in the NAI's self-regulatory regime from advertising technology companies, consumers also showed more engagement with online privacy as exhibited by the increased visits to the NAI's website. In 2015 the NAI website welcomed over 8.2 Million unique visitors, up from 5.6 Million in 2014.

9 *Cross-Device Tracking: An FTC Workshop,* FTC (Nov. 16, 2015), www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking [hereinafter FTC Cross-Device Workshop].

10 *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices*, Digital Advertising Alliance (Nov. 2015), *available at* www.aboutads.info/sites/default/files/DAA_Cross-Device_Guidance-Final.pdf.

# THE NAI COMPLIANCE PROGRAM

## APPROVING NEW MEMBER COMPANIES—COMPLIANCE BEGINS EVEN BEFORE COMPANIES JOIN THE NAI

Companies interested in NAI membership cannot simply join the NAI; they must commit to compliance. Compliance efforts begin even before a company becomes a member. At least two members of NAI staff, consisting of lawyers and technologists, evaluate each applicant's business model and privacy practices. These reviews focus on a company's application questionnaire and privacy disclosures, as well as data collection, use, retention, and sharing practices to ensure these are consistent with the Code. Additionally, NAI staff with technical training evaluates the applicant's consumer choice mechanisms and data collection practices. NAI staff then conducts interviews with high-level employees at the applicant company wherein the applicant is subject to further questions, including resolution of any potential discrepancies in their application materials, or business practices that may be inconsistent with the Code.

"We find the NAI annual compliance review process an essential part of our privacy program – the review helps us apply the Code to our business without trying to navigate through the compliance process alone."

Diana Olin, Senior Legal Counsel, YuMe

An applicant that wishes to complete the application process must work with NAI staff to help bring its relevant services and products into a position to be in compliance with the Code. NAI staff evaluates each applicant's practices and disclosures in order to highlight those that need to be addressed before the company can become a member of the NAI. Though some companies are able to attain membership within a few weeks, this assessment can often be a months-long process, with the NAI providing guidance and suggestions about compliance at every step. Many applicants make substantial revisions to their public privacy disclosures in order to provide the full level of notice required by the Code. Typically, NAI staff provides technical guidance to help an applicant develop a fully functional Opt-Out Mechanism[11] that can both meet the Code's requirements and be compatible with the NAI opt-out page. At times, applicants have abandoned or dramatically revised entire lines of business that did not, or could not, meet the requirements of the Code.

Once this pre-membership review is completed, NAI staff submits a recommendation for membership to the NAI Board of Directors. The NAI Board of Directors is comprised of seasoned attorneys and compliance executives from 14 leading member companies. The Board reviews each application, often requesting additional information from an applicant, before voting on acceptance of a new member. Therefore, each potential member is reviewed by both NAI staff and the Board. This review process helps establish that an applicant's administrative, operational and technical capabilities can comply with the requirements of the Code before the applicant may claim membership in the NAI.

In 2015, thirteen companies[12] completed the application process and were approved for membership by the Board.

11 Opt-Out Mechanism is defined under the Code as "an easy-to-use mechanism by which individuals may exercise choice to disallow Interest-Based Advertising with respect to a particular browser or device" (§ I.J.).

12 The following 13 companies went through the new member application process and became NAI members in 2015: AcuityAds, BlueCava, Drawbridge, Ezakus, Kargo, Optimatic, Tagular, BAM, Parrable, Yieldmo, Circulate, EyeView, LinkedIn.

### At the close of the 2015 compliance review period, the NAI Board consisted of:

**Alan Chapell:** President of Chapell and Associates, representing Audience Science

**Alice Lincoln:** Vice President of Product Management & Data Governance, MediaMath

**Andrew Pancer:** Chief Operating Officer, Dstillery

**Ari Levenfeld:** Senior Director of Privacy and Inventory Quality, Rocket Fuel, Inc.

**Brooks Dobbs:** Chief Privacy Officer, KBMGroup

**Charles Simon:** Product Manager for Privacy, Oracle

**Dave Fall:** General Manager and Senior Vice President of Operations, Tapad

**David Wainberg:** Vice President, Privacy & Policy Counsel, AppNexus

**Douglas Miller:** Vice President and Global Privacy Leader, Aol Advertising

**Estelle Werth:** Global Privacy Officer, Criteo

**Jason Bier:** Chief Privacy Officer, Conversant

**Matthew Haies:** Senior Vice President & General Counsel, Xaxis

**Shane Wiley:** Vice President of Privacy & Data Governance, Yahoo!

**Ted Lazarus:** Director, Legal, Google

# MONITORING OF MEMBERS

## NAI Technical Monitoring

Once companies demonstrate their ability to comply with the Code, and become members of the NAI, they must remain in compliance so long as they maintain their membership. One way the NAI helps facilitate this process, even in between annual compliance reviews, is through its technical monitoring suite. Through continuous development, the NAI has integrated its Opt-Out Scanner and Privacy Disclosures Scanner into a single issue-tracking system that allows staff to flag potential issues for review or investigation.

One of the main benefits of these monitoring tools is their ability to help NAI staff spot and remedy potential problems quickly, thus enabling the NAI to address concerns with members before they become widespread and affect large numbers of consumers. In 2015 the NAI's proprietary monitoring software flagged an average of six items per week warranting further investigation or testing. These instances included extensive revisions to privacy policies, new opt-out behavior, and apparent errors by the tools in accessing certain privacy disclosures. Upon further review, NAI staff was typically able to confirm that these flags did not point to material violations of the Code, and that all the required disclosures were still present on the member companies' websites. For example, a flag may have been raised when a privacy policy appeared to be inaccessible, though further investigation demonstrated that the disclosures in question continued to be accessible to consumers at a different location.

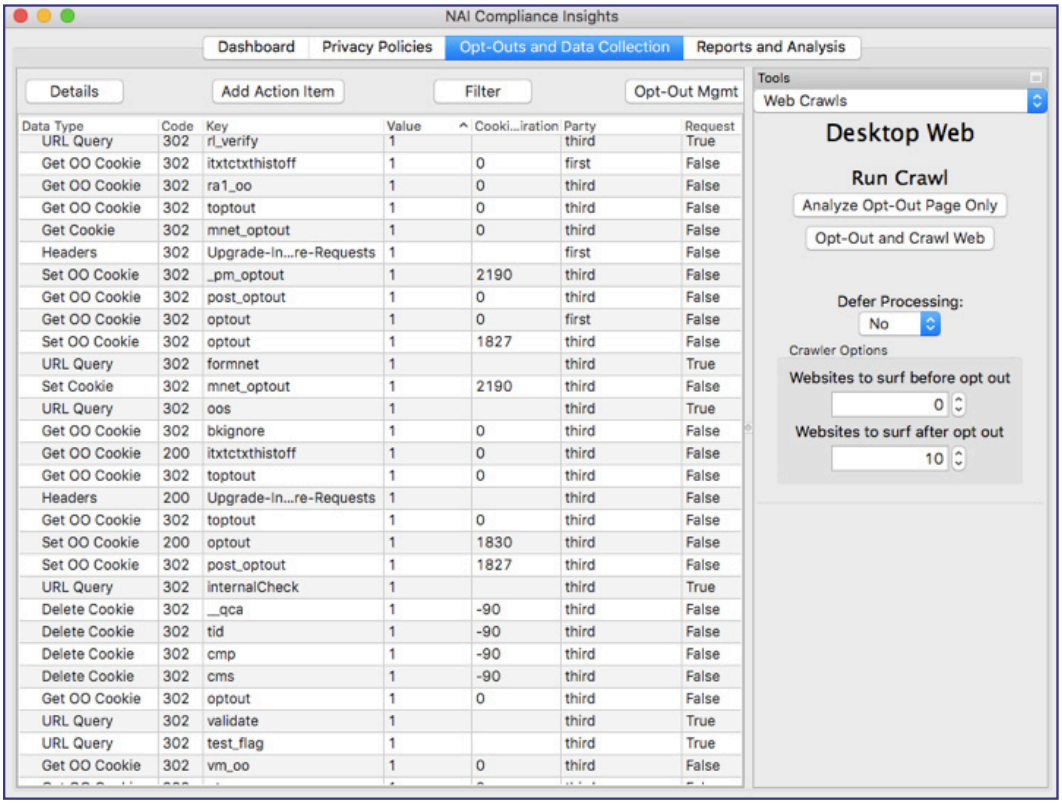
On a number of occasions, however, the NAI's monitoring tools spotted actionable issues that could have resulted in Code violations if left unaddressed. Every such actionable issue that was identified through the use of the NAI monitoring tools was resolved shortly after it was disclosed to the member company by NAI staff. As in the prior year, none of these issues were considered to be material non-compliance with the Code because the underlying issues were resolved quickly, were found to be unintentional, and affected a limited number of consumers. As has become commonplace, many members experiencing such technical problems went on to develop and provide additional technical and administrative checks to help prevent similar issues from recurring, and those processes are continually tested through the NAI's monitoring tools.

In 2015 the NAI further developed its in-house tool, scanning through 300 web pages to monitor the privacy disclosures of existing members and applicants for changes.

In addition to flagging major potential problems, these tools also helped NAI staff flag an average of ten minor changes per week, such as those resulting from members adding a new product or technology. For example, companies tended to add new privacy disclosures in anticipation of product launches, prompting questions about data flows during annual compliance reviews. As in the past, the compliance staff's interactions with members gives them knowledge and understanding of new business practices that may have arisen throughout the year that affect member activities and privacy considerations. This process continues to aid NAI staff in incorporating new concepts into the following year's annual compliance reviews.

## Opt-Out Testing

The NAI administers two types of ongoing reviews of member opt outs: routine manual checks of the NAI's opt-out page and more detailed, in-depth scans. Through the routine manual testing, NAI staff use the NAI opt-out page and look for errors, such as companies that experience failures and issues in loading the opt-out page.



The NAI also scans members' opt-outs through proprietary software.[13] The Opt-Out Scanner collects information about the cookies set via the NAI opt-out page and generates a short report, helping staff to recognize when required opt-out cookies are not set or if the opt-out cookie's duration is too short. Such problems are rare and can result from incomplete server migrations or the launch of new products and services.

This holistic approach helps the NAI to address potential problems with member Opt-Out Mechanisms. The routine opt-out checks aided in spotting issues such as opt-out malfunctioning and the Opt-Out Scanner helped to reveal changes in members' use of known domains or cookies. Additionally, the NAI receives consumer emails regarding specific functionality issues that are difficult to identify with in-house testing, such as temporary malfunctions on servers that affect only certain cities. The combination of monitoring, daily manual testing, and review of consumer emails helped the NAI and its members limit opt-out downtime. Through these processes and tools, opt-out issues were resolved before resulting in material non-compliance with the Code.

### Privacy Disclosures Scanner

In 2014, NAI introduced an in-house tool which now scans over 300 privacy policy disclosures of members and applicants for changes to those disclosures. The Privacy Disclosures Scanner continues to scan web pages for modifications, as well as errors in accessing those web pages. As in the past, these scans helped NAI staff identify a variety of potential compliance issues, including incomplete or missing disclosures and broken links or non-conforming opt-out mechanisms. NAI staff worked with members to promptly address any inconsistencies.

The Privacy Disclosures Scanner helped bring numerous business model changes to the attention of NAI staff, such as new products offered by NAI member companies, and acquisitions of new brands and business lines. Because disclosures in privacy policies usually occur in anticipation of the launch of a new product, spotting these changes allowed NAI staff to help members evaluate how the Code applies to these new products and offerings. As in the past, knowledge of new business models that may have arisen throughout the year helped further develop the NAI's monitoring tools and aided NAI staff in incorporating new concepts into the following year's annual compliance reviews.

Continuing a trend from the previous year, many of the changes to members' privacy disclosures were positive. In other words, many of the changes were the result of members responding to action items and feedback provided by the NAI staff, members proactively disclosing a new product or technology, or members making changes to privacy policies in reaction to a change of legal requirements.

13 Under the Code, each member is required to provide and honor the consumers' choice to disallow IBA data collection and use by a member on a particular browser through an Opt-Out Mechanism (§ II.C.2.).

To the extent there were any deletions or changes of language in member privacy policies required by the Code, these were not considered to be material violations because revisions were made to comply with the Code within a reasonable time from NAI staff's notice to the member. NAI staff continues to acknowledge that members face the difficult task of explaining to consumers in a clear yet meaningful manner, through their privacy disclosures, what data they are collecting and using for IBA. Members strive to have accurate privacy policies. NAI also recognizes that members must balance the need to be concise with the need to provide thorough disclosures. NAI staff applies its extensive knowledge of the industry, understanding of the Code, and expert judgment, from an NAI Code perspective, in determining the relative adequacy of the disclosures in a member's privacy policy.

## Investigating Consumer Communications

### NAI Website

The NAI website provides a centralized mechanism for consumers to ask questions and raise concerns about members' compliance with the Code (§ III.C.1.).

In 2015, NAI received and reviewed approximately 5,700 consumer queries through its website, approximately 400 via telephone, and several letters through postal mail.

This is a considerable reduction from the 9,000 queries received in 2014, and may reflect updates allowing the NAI opt-out tool to function in the presence of common ad blocking software.[14] NAI staff determined that, as in the past, the majority of the inquiries received did not pertain to issues within the scope of the NAI's mission. For example, many emails asked questions about junk e-mail, or were attempts to reach the publishers of specific websites, or other issues not covered by the Code.

**In 2015, NAI received and reviewed over 6,000 consumer queries.**

Less than 40 percent of consumer inquiries were related to the NAI or member companies, and the vast majority of these inquiries were requests for assistance in troubleshooting technical issues with IBA opt outs. NAI responded with guidance explaining how consumers can use the opt-out page when browser controls blocked third-party cookies, and descriptions of how ISP/workplace Internet filters or anti-virus software could prevent opt-out cookies from being set on the consumer's browser. In several instances, consumers notified the NAI of specific opt-out issues, and helped confirm potential problems flagged through the use of the NAI's monitoring tools.

14 Consumers using ad blockers previously saw more frequent errors on the NAI's opt-out page because the ad blockers prevented most member companies from reading or saving a user's opt-out preferences. To solve these problems, the NAI obtained an exception from a major ad blocking list for its opt-out page.

In 2015, consumer inquiries led to one NAI compliance investigation, which concluded that a misunderstanding had caused concern among consumers about a member company's cookies returning after an opt out. The NAI's investigation determined that ultimately these were first-party cookies, set by the member company on its own website, and were not related to the member company's IBA activities.

In summary, NAI staff determined that consumer communication received by the NAI in 2015, through email, phone, letter or the website that were conducive to resolution had been resolved within a reasonable timeframe and any allegations of member non-compliance with the Code were non-material.

### Consumer Question Mechanisms

During 2014, NAI launched a program to review members' sites and confirm that they provide mechanisms through which consumers may submit questions or complaints directly to the member (Code § III.C.2.). NAI staff repeated this process in 2015 as part of the Annual Compliance Review.

NAI staff tested members' compliance with section III.C.2 of the Code by reviewing their sites to ensure that they offered a mechanism for consumers to submit questions or concerns about the company's collection and use of data for IBA. NAI staff found that all evaluated member companies provided an email address, web based form, or troubleshooting guide tied to a forum for consumers to use if they wished to ask questions about the company's privacy practices.

NAI staff also independently tested members' responses to consumer questions sent through these question mechanisms. NAI sent test emails to member companies with standardized questions about opting out of IBA.

In those instances where NAI staff did not receive a response, or received a response that was inadequate, the evaluated member companies were notified of the problem. All of the companies that received such notifications from NAI staff confirmed that they worked to resolve the issues, which were often caused by junk email filtering. Importantly, these companies also provided a link to the NAI's opt-out page without interruption, thus ensuring that consumers could still pose questions and send complaints through the NAI's own consumer question mechanism which provides a back-up means for consumers to voice privacy concerns regarding member companies' data collection and use for IBA.

### Investigating Other Allegations and Complaints

In addition to the NAI's own monitoring and research, NAI staff also scrutinizes a variety of other sources for potential instances of member non-compliance, including published articles, public allegations by privacy advocates, complaints to NAI by third parties or other NAI members, and investigations by other regulatory bodies. In 2015, NAI staff conducted two investigations based on such allegations of potential non-compliance with the Code. These investigations included notice of the use of non-cookie technologies and the use of Sensitive Data for IBA.

The investigations and reviews during this compliance period included the examination of the alleged practices under the Code, discussions with relevant member companies, and the review of public and non-public facts. In the two cases investigated during this period, NAI staff, or the NAI Board of Directors, based on a recommendation from the Compliance Committee, determined that the member companies' activities did not constitute a violation of the Code, and therefore sanctions were not appropriate.

# ANNUAL REVIEW

As part of their membership obligations, NAI members are required to annually undergo reviews of their compliance with the Code by NAI compliance staff.

During the 2015 annual compliance review, NAI staff reviewed the 84 companies that were members from January 1 through December 31, 2015.[15] These members will be referred to as "evaluated member companies" throughout this report. Those members that joined the NAI after January 1, 2015[16] were already subject to review during the calendar year as part of the on-boarding process, and therefore were not part of the 2015 annual compliance review. Those members will be assessed again during the 2016 annual review process.[17]

## Training

In 2015, the NAI conducted a number of training sessions for its members, including education about the Code as well as training webinars on the Guidance on Non-Cookie Technologies.

The NAI provided three training webinars designed to educate members about the 2015 Code Update. During these webinars, NAI staff explained the key requirements of the updated Code, which went into effect on June 1, 2015. In particular, NAI staff reviewed the differences between the 2013 Code and the 2015 Code Update, and other requirements of the Code. These presentations were intended to supplement the general training NAI staff provided members on individual policy issues throughout the year.

15 The following companies were reviewed in 2014 but are no longer members of the NAI:
- a LiveRamp, Brilig, Mixpo, Zedo, Batanga Networks, IDG Tech Network, Rich Relevance, and eBay Enterprise represented to NAI staff that they did not engage, or ceased engaging, in IBA activities. These companies did not complete the 2015 annual compliance review.
- b MLN Advertising was absorbed by NAI member AppNexus, Cognitive Match was absorbed by NAI member Magnetic, and Legolas was absorbed by NAI member Undertone. These three companies ceased independent operations and were therefore not evaluated independently of their parent companies during the 2015 annual review process.
- c Bizo was absorbed by LinkedIn, and ceased independent operations. Bizo was not evaluated independently of LinkedIn during LinkedIn's new member application process in 2015.
- d IgnitionOne absorbed the membership of its wholly owned subsidiary Netmining, and as a result Netmining's operations were not reviewed independently of its parent company.

16 *See* FTC Cross-Device Workshop, *supra* note 9.

17 NAI staff makes an effort to review new member companies first, during the subsequent annual review, in order to minimize the time between a member's initial membership application review and its first annual compliance review.

## Evaluated Member Companies

33Across

Accuen

Adara

Adblade

AddThis

AdRoll

Aggregate Knowledge

AOL Advertising

AppNexus

Atlas Solutions

AudienceScience

Bazaarvoice

BlueKai

Brightroll

Chango

ChoiceStream

Collective Media

Conversant

Criteo

Cross Pixel

DataLogix

DataXu

Datonics

Defy Media

Dstillery

eXelate

Exponential Interactive (formerly Tribal Fusion)

Eyereturn Marketing

Flashtalking

Gamut

Google

GumGum

Ignition One/ Netmining

Index

Innovid

Intent Media

KBM Group

Krux Digital

LiveRail

Lotame Solutions

Madison Logic

MAGNETIC

Markit On Demand

MaxPoint Interactive

Media Innovation Group

Media.Net

MediaForge

MediaMath

Microsoft Advertising

Mode Media

NetSeer

Neustar

OwnerIQ

PointRoll

Proclivity Media

PubMatic

Pulsepoint

Quantcast

RadiumOne

RhythmOne (formerly Burst Media)

Rocket Fuel

RUN

ShareThis

Simpli.fi Holdings

Sizmek

Specific Media

SteelHouse

Tapad

TellApart

the Rubicon Project

The Trade Desk

Triggit

TruEffect

TubeMogul

Turn

Undertone (including Legolas Media)

Varick Media Management

Vibrant Media

Videology

Vindico

Xaxis

Yahoo

YuMe

[x+1]

> "The NAI compliance process helps me and my team put out questions to our colleagues around our company's data collection and use on an annual basis as our business changes and grows."
>
> Michael Blum, Senior Vice President, Business and Legal Affairs, Quantcast

Additionally, NAI staff provided members with four training webinars to address the requirements of the NAI's Guidance on Non-Cookie Technologies for IBA. The goal of these webinars was to help member companies ensure that they successfully deploy and maintain non-cookie technologies in a manner consistent with the Code and the Guidance. NAI staff also provided members with technical guidance regarding the functionality of the NAI's updated consumer choice page, and explained how member companies can integrate their technologies with the new features provided by the NAI.

## Written Questionnaire and Supporting Documentation

Evaluated member companies submitted written responses to an updated 2015 compliance questionnaire. The questionnaire required evaluated member companies to describe their business practices and policies in juxtaposition to the requirements created by the Code. Where relevant, the questionnaire also requested that evaluated member companies provide supporting documentation such as sample contract language, links to specific disclosures, and training materials. Consistent with prior reviews, this questionnaire covered such issues as the collection and use of data for IBA purposes; policies governing those practices; contractual requirements imposed on business partners concerning notice and choice around IBA activities;[18] other protections for data collected and used for IBA purposes, such as data retention schedules; and processes for oversight and enforcement of contractual requirements. At the end of the compliance review period, the NAI required members to sign attestation forms to confirm that their responses continued to be accurate to the best of the member's knowledge.

A minimum of two members of NAI staff reviewed each evaluated member company's submitted materials to assess compliance with the Code. NAI staff reviewed responses to the NAI's extensive questionnaire and representations of business practices as set forth in the evaluated member company's public and non-public materials. These materials generally included news articles, the member company's website, privacy policy, terms of service and advertising contracts.

18 If a member has an agreement with a partner to collect data on the partner's site where it collects and uses data for IBA purposes, the member is obligated to require through its contractual provisions that the partner provide a link to the NAI website on the partner's site (Code § II.B.3.).

## Interviews

Following the review of questionnaire submissions and other supporting materials, at least two members of NAI staff interviewed representatives from evaluated member companies. These interviews were conducted primarily with high-level management and engineering employees. NAI staff explored the business practices of evaluated member companies, and requested additional clarification on the calls in the event that questionnaire answers were incomplete, vague, unclear, or seemingly inconsistent with the NAI's own review of a company's business model. As appropriate, the NAI compliance team also queried technical representatives about data flows, opt-out functionality, data retention policies and procedures, and technologies used for IBA.

**NAI member companies include all of the comScore Top 10 Ad Networks.**

These interviews provided the compliance team with additional in-depth insight into evaluated member company businesses and the industry in general, especially as new business models and technologies continue to emerge. This integrated view of the industry, resulting from direct engagement with nearly 100 companies comprising a significant portion[19] of the third party advertising technology ecosystem, augments the staff's ability to flag potential privacy issues to members, Code violations in general, and shapes NAI staff recommendations regarding future guidance and policies.

These interviews also offered an opportunity for the compliance team to provide best practice suggestions for evaluated member companies. During these calls, staff reminded evaluated member companies to perform frequent checks of their Opt-Out Mechanisms to ensure they function correctly. NAI staff also suggested steps evaluated member companies should take when working with third party data providers, to help ensure that data comes from reliable sources. The NAI often provided recommendations on alternative language for privacy disclosures, based on NAI staff's collective experience of reading hundreds of member and website publisher privacy policies. The compliance team provided extensive feedback to evaluated member companies to help them improve messaging regarding opt-out successes, or potential opt-out failures due to browser level controls. The NAI recommended that evaluated member companies provide a clear, visual confirmation of a successful opt out or a corresponding error message if a consumer's browser prevented an opt-out cookie from being set.

## Attestations

After the completion of the questionnaire and interview process, and as a final step in the annual compliance review, evaluated member companies were required to attest in writing to their ongoing compliance with the Code. These companies were also required to attest to the veracity of the information provided during the review process.

19 *See comScore Ranks the Top 50 U.S. Digital Media Properties for February 2016,* comScore (March 21, 2016), *available at* www.comscore.com/Insights/Rankings/comScore-Ranks-the-Top-50-US-Digital-Media-Properties-for-February-2016 (NAI member companies comprise all of the Top 10, and 18 of the Top 20 Ad Networks).

# 2015 ANNUAL REVIEW FINDINGS

The Code requires the NAI to publish the results of its annual review, providing an opportunity for the NAI to summarize members' compliance with the Code and NAI policies (§ III.B.3). The following section presents the findings of NAI staff with respect to the 2015 annual review. This section also more fully summarizes the obligations imposed by the Code, but does not restate all principles set forth in the Code, and as such it should not be relied upon for that purpose. The full Code, including definitions of relevant terms, can be found through the links provided in this report.

# EDUCATION

The Code stipulates that members should use reasonable efforts to educate consumers about IBA, and requires members to maintain an NAI website to educate consumers (§ II.A.). It is key that the NAI provide a centralized education page that members may point to, implementing uniform terminology to help explain what can be a complex ad tech ecosystem to consumers. Accordingly, all members collectively educate consumers through the provision of the NAI website, which serves as a centralized portal for explanations of IBA and associated practices, as well as for providing consumer access to choice mechanisms. Members provide links to the NAI through their own websites, where consumers may also learn about the IBA. In 2015, evaluated member companies continued to meet this obligation to collectively educate consumers about IBA and their available choices.

**Evaluated member companies estimate that they have collectively provided billions of impressions to the NAI's educational campaign.**

Evaluated member companies also continued to promote the NAI's education pages through a digital advertising campaign, estimating that they've donated billions of impressions to the campaign. The NAI educational campaign helped lead to over 5.3 million page views of the NAI education pages in 2015, an increase of nearly 20% over the prior year.

The NAI is also planning updated consumer education materials, reflecting a shift in the industry toward mobile ecosystems, non-cookie technologies, and the linking of devices for advertising purposes. The NAI plans to launch these updated materials in 2016 in order to educate consumers about the privacy implications of the latest developments in these technologies, and the most recent updates to NAI guidance.

Beyond maintaining a centralized consumer education page, the Code further suggests that member companies should individually educate consumers about IBA and the choices available to them (§ II.A.2.). NAI staff found that evaluated member companies provided information regarding the technologies used for IBA and a clear link to a consumer choice page. In addition, NAI staff found that many evaluated member companies provided separate consumer education content outside their privacy disclosures or opt-out pages. These pages were dedicated to explaining the evaluated member's IBA activities and providing consumers with an easy to locate choice mechanism.

**The NAI education campaign helped lead to over 5.3 million page views on the NAI education pages in 2015, or an increase of nearly 20% over the prior year.**

Several NAI members also play key roles in the Federation for Internet Alerts (FIA),[20] which uses advertising technology for the common good, distributing life-saving information to the right viewers at the right time, including missing child Amber Alerts and severe weather warnings. Leveraging advertising technology for public service is an extension of the broader education efforts undertaken by NAI members.

Through their contributions to the NAI's education campaign, as well as through informational material on their own websites, evaluated member companies collectively invested considerable effort and resources to educate consumers about IBA, while also using advertising technology to benefit society.

# TRANSPARENCY AND NOTICE

## Member Provided Notice

Section II.B.1. of the Code requires members to provide "clear, meaningful, and prominent notice" on the member's website describing their IBA and/or ADR practices.

### Prominent Notice

In 2015 NAI staff reviewed the websites of evaluated member companies to determine if they met the obligation to provide "prominent" notice. The purpose behind this obligation is to help ensure that consumers can quickly and easily find a link leading them to information about a member company's IBA activities and to exercise choice regarding IBA at their discretion.

As a result of ongoing educational efforts during prior compliance reviews, NAI staff found that at the time of their 2015 reviews, all evaluated member companies provided an easy to find link to privacy disclosures in the footer or header of their websites.

The vast majority of evaluated member companies continue to offer a separate and obvious link to an Opt-Out Mechanism, a prominent link to the NAI opt-out page, or a "Your AdChoices" link. Interviews with their representatives demonstrated that evaluated member companies understand it is key for consumers to be able to quickly and easily locate information regarding these companies' IBA activities.

20 *See* Federation for Internet Alerts (2016), www.internetalerts.org.

All evaluated member companies provided an easy-to-find link to privacy disclosures.

### Clear and Meaningful Notice

The Code requires that evaluated member companies publicly disclose their IBA and ADR data collection and use practices in an understandable manner. This includes, as applicable, providing a description of the IBA and/or ADR activities undertaken by member companies; the types of data they collect; their use and transfer; a general description of the technologies used by members for IBA, and/or ADR activities;[21] a data retention statement; and an Opt-Out Mechanism. Finally, the Code requires members to disclose that the company is a member of the NAI and adheres to the Code (§ II.B.1.f.).

During the 2015 annual review, NAI staff assessed the privacy policies and disclosures of evaluated member companies in juxtaposition with current IBA practices as described in each company's annual interview, its corporate site, annual compliance review questionnaire, business model changes discovered through ongoing monitoring, and news articles.[22] The NAI offered evaluated member companies suggestions to make privacy disclosures clearer and easier to understand. Further, NAI staff noted that evaluated member companies amended their privacy policies in 2015 to reflect the use of newer technologies for IBA and ADR, and to provide more information about data collection and use on mobile devices.

### Pass-On Notice

Although the NAI's self-regulatory program applies only to its members, NAI members can in turn help ensure, through contractual requirements with website publishers, that consumer-facing websites post information about IBA data collection and use (§ II.B.3.). These contractual notice provisions are important as they help ensure consumers are provided with notice at the point of data collection, including in instances where the ad icon or other in-ad notice is not available because IBA-based ads are not offered on a given site. This would be the case in instances where the publisher site is engaged in Retargeting, for example. Based on a review of evaluated member companies' sample partner contracts, the NAI found that evaluated member companies overwhelmingly included such contractual requirements when working directly with publishers.[23]

As part of NAI members' overall efforts to promote transparency in the marketplace, members should also make reasonable efforts to enforce the above contractual requirements and to otherwise ensure that all websites where they collect data for IBA purposes furnish consumer notice (§ II.B.4.).

21 Members are not required to disclose the technologies they use for IBA and/or ADR with the level of specificity that would reveal their proprietary business models. However, members are expected to provide general descriptions of the technologies they are using for IBA and/or ADR.

22 With the creation of the Privacy Disclosures Monitoring Tool, the NAI can now monitor member privacy disclosures to ensure that members do not inadvertently delete language required by the Code.

23 The NAI determined that some evaluated member companies did not collect data, but instead facilitated others' collection of data for IBA purposes, such as advertising technology platforms. The NAI encourages, but does not require, that these members ensure that proper notice is provided where their technology is used to collect data for IBA purposes. The NAI found during the compliance review that many such evaluated member companies nonetheless provided such notices.

As in the past, the NAI found that many evaluated member companies continued to conduct due diligence on websites where they sought to conduct IBA activities prior to engaging in IBA activities on those sites. Some evaluated member companies trained their sales teams to evaluate website notice when onboarding new partners, while other member companies did not do business with websites unwilling to include the notice.

Many evaluated member companies also continued to perform random follow-up checks on all, or a cross-section, of their partner sites. Many evaluated member companies reviewed thousands of publisher sites for the required disclosures. Evaluated member companies then reached out to those partner websites that did not include any or all recommended elements of the public privacy disclosures. A few individual evaluated members reported that they terminated relationships where a partner was unwilling to provide the required disclosures.

NAI staff provided guidelines for procedures to check on partner sites, in a manner that was feasible even for members with limited resources for those evaluated member companies that did not have any processes in place for ensuring that website partners furnish the required disclosures. In addition, the NAI provides its members with a static web page as a reference point for pass-on notice requirements, making it easier for member companies to explain this Code requirement to customers.

### Enhanced Notice Requirement

The Code requires that members provide, and support the provision of, notice in or around advertisements informed by IBA, thus providing just-in-time notice by NAI members to consumers, offering yet another means by which consumers can be informed of members' IBA activities, and the choices available to them. In 2015, NAI members continued to lead industry efforts to provide real-time notice and choice to consumers in and around the ads delivered to them by serving a form of enhanced notice, such as the YourAdChoices icon which is served at a rate of one trillion times per month.[24] The NAI found that those evaluated member companies who lacked the ability to include the standard industry icon or other form of enhanced notice promoted the provision of such notice by configuring their systems to support that capability. Those evaluated member companies that offer technology platforms, and only facilitate the collection of data by their clients for IBA, provided their clients with the ability to include this notice on their advertisements through the platform settings.

24 Because of technical challenges with providing enhanced notice in video advertisements, the NAI is not enforcing this requirement in video advertisements at this time. The NAI will make a formal notice before enforcement once the technological challenges are overcome.

## Health Transparency

NAI members are required to publicly disclose the standard interest segments they use for IBA that are based on health-related information (Code § II.B.2.). In this context, "standard segments" are those profiles based on health-related information that are pre-packaged and offered for IBA purposes by a member. Standard segments do not include those profiles offered to advertisers for IBA purposes that are created or customized on a request basis, for a specific advertiser or advertising campaign. This Code requirement calls for members to disclose not only sensitive health segments (such as an inference that a consumer may be interested in products or treatments for cancer, mental health conditions, or sexually transmitted diseases, among others), but also inferred interests in non-sensitive topics as well, such as skin care, diet, or fitness. Because the relative sensitivity of a health condition or treatment is often subjective, the goal behind this broad disclosure requirement is to allow consumers to make their own educated decisions about whether to opt out of the collection and use of data for IBA by a specific member company, dependent on the type of health-related targeting the company engages in. This disclosure requirement continues to be separate and distinct from the Opt-In Consent[25] requirement for IBA uses of sensitive health data discussed in the next section.

Based on responses to the questionnaire, individual interviews, and NAI staff review of evaluated member companies' websites, as well as through automated monitoring, NAI staff found that overwhelmingly, evaluated member companies complied with this requirement, often in a variety of formats. Some members disclosed all standard interest-based segments made available to partners, whether or not the segments were related to health topics. Several members provided preference managers or other tools that not only allowed consumers to view a list of available interest segments, but also enabled granular control for those consumers that did not wish to be targeted based on inferences about these segments. Others listed all health-related segments through links from their privacy or marketing pages. The NAI agrees that there are a variety of means for this information to be provided in a manner that complies with the Code, and does not require that members use a specific format. Indeed, NAI staff noted that compliance with this requirement continues to improve, and that evaluated member companies continue to make more complete, accurate, and accessible disclosures as a result of discussions with NAI staff.

NAI staff found that many evaluated member companies do not offer standard interest segments associated with health topics.[26] However, some evaluated member companies did offer custom, non-sensitive health segments for individual advertising campaigns. NAI staff continues to encourage those members to publicly provide examples of such customized segments to better educate the public about their activities.

25 Under the Code, Opt-In Consent means that "a user takes some affirmative action that manifests the intent to opt in" (§ I.I.).

26 Many evaluated member companies did not employ "standard" interest segments at all, but rather engaged only in practices such as retargeting, or custom segmentation.

There were over 7.6 million visits to the centralized, NAI opt-out page in 2015.

# USER CONTROL

Consumer choice is one of the pillars of the Code. The level of choice that NAI members must provide to consumers is commensurate with the sensitivity and intended use of the data. The Code's framework continues to recognize that different categories of data may present different levels of potential risk, and therefore require different levels of user control.

## Presence of Opt-Out Mechanisms

NAI members are required to provide consumers with the ability to opt out of the collection and use of Non-PII[27] for IBA purposes, including Retargeting. Member companies must provide an Opt-Out Mechanism in two discrete locations: on the member's website and on the NAI website (Code § II.C.1.a.). In 2015 the NAI independently confirmed that evaluated member companies provided an Opt-Out Mechanism both on their own website and on the NAI consumer website.

Through the use of its proprietary monitoring tools, NAI staff noted that occasionally evaluated member companies opt-out links, in their privacy policies or elsewhere on their sites, may not have been fully functional, though these member companies continued to offer functional Opt-Out Mechanisms elsewhere on their sites (e.g., the evaluated member companies offered an opt-out link leading consumers to the NAI opt-out page). In these instances, evaluated member companies worked with NAI staff to quickly fix the broken links. Because of manual testing during annual compliance reviews, as well as ongoing monitoring using the NAI's automated tools, NAI staff continues to help evaluated member companies to identify broken or malfunctioning links in a prompt manner, thus minimizing the effect of these issues on consumers.

27 Non-PII is data that is linked or reasonably linkable to a particular computer or device. Non-PII includes, but is not limited to, unique identifiers associated with users' computers or devices and IP addresses, where such identifiers or IP addresses are not linked to PII. Non-PII does not include De-Identified Data" (Code § I.E.).

## Honoring Opt-Out Mechanisms

The Code requires that members honor the user's choice as to the particular browser when a user has opted out of IBA (§ II.C.2.). A member must stop the collection and use of data for IBA while an opt-out preference is set and stored on a given browser.[28]

In 2015 NAI staff took multiple steps to help evaluated member companies confirm their compliance with this requirement. Evaluated member companies filled out a detailed compliance questionnaire regarding the functionalities of their Opt-Out Mechanisms, including listing the types of technologies they used for IBA. This questionnaire asked evaluated member companies to provide the name, value, domain, and purpose of every cookie they continued to set following an opt out. As part of the annual compliance review, NAI staff continued to manually review each opt-out cookie to independently evaluate the accuracy of the information submitted in the questionnaire. For example, NAI staff reviewed the behavior of opt-out scripts, the names, value, and lifespans of opt-out cookies, as well as the names and values of any potentially unique cookies that were used while an opt-out cookie was present on the browser. Of those evaluated member companies that continued to set cookies with unique identifiers while an opt out was present on a browser, all confirmed during the annual compliance review interviews that such use was for non-IBA purposes only, such as for analytics, frequency capping, and attribution, as permitted by the Code.

**NAI staff examined the behavior of over 23,200 data elements, including cookies, Javascript files, and URL query strings of its evaluated member companies.**

As has become NAI practice, these tests also looked for opt-out functionality issues caused by blocking cookies and certain compatibility requirements on browsers. This review complements, but does not replace NAI staffs' regular technical monitoring using the Opt-Out Scanner. Further, in 2015 NAI staff considerably expanded its reviews of non-cookie technologies, enhancing the existing review program for cookie-based data collection and use. The questionnaire responses, combined with manual testing by NAI staff, indicated that evaluated member companies stopped using data for IBA purposes in the presence of an opt-out cookie.

28 Members may continue to collect data for other purposes, including ADR. For example, members may continue to collect data from a browser to prevent fraud or to verify that an ad was displayed to that browser.

In a review of the expiration dates of opt-out cookies set by evaluated member companies, NAI staff noted that these cookies had expiration dates at least five years into the future, as required by the NAI, and often were set to last considerably longer than this mandated minimum.[29]

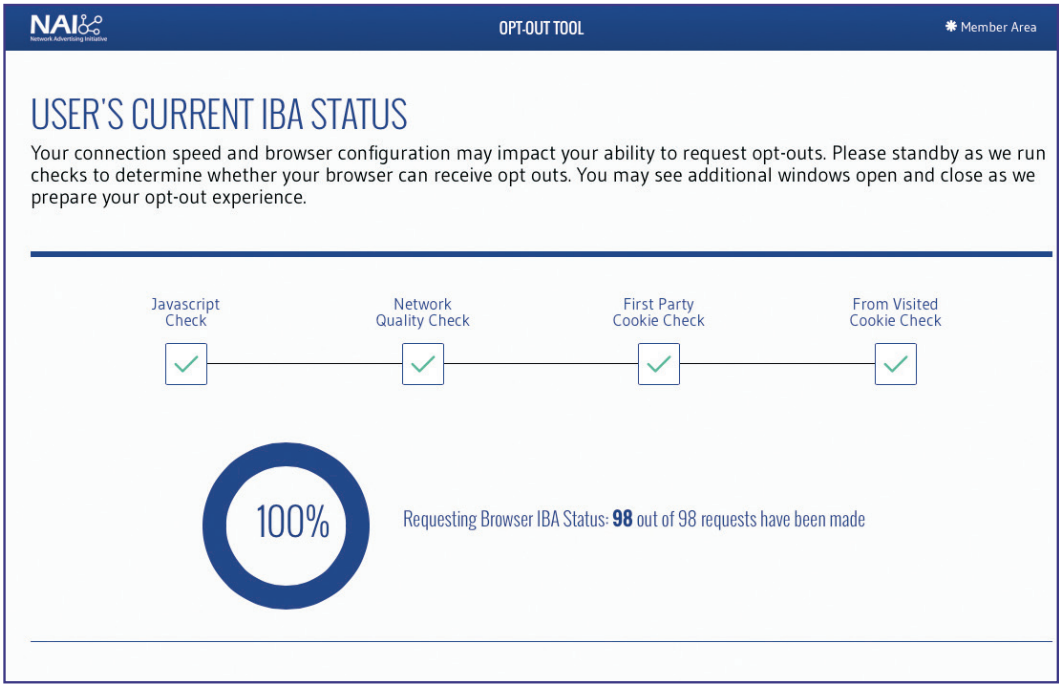
Based on the annual questionnaire answers, the NAI further found that evaluated member companies continued to employ sophisticated systems and policies in place to help verify the effective operation of their opt-out technology. Some evaluated member companies conducted manual testing of their own opt outs, while others employed automated monitoring tools, or conducted regression tests for any software or code changes on their servers, and all are required by the Code to monitor consumer complaints, about opt-out functionality, submitted through their websites. On several occasions, NAI staff encouraged evaluated member companies to perform additional and more frequent testing of their Opt-Out Mechanisms and suggested methods successfully used for this purpose by other members.

NAI staff's manual reviews of member Opt-Out Mechanisms, compliance questionnaire responses, and telephone interviews, supplemented by automated technical monitoring, indicated that evaluated member companies' Opt-Out Mechanisms appeared to function as intended and that potential technical problems resulting in downtime of an opt out were quickly identified and resolved.

29 *Understanding Online Advertising: Frequently Asked Questions*, NAI, *available at* www.networkadvertising.org/faq/#n178.

## Technologies Used for IBA

Though the Code is intended to be technology-neutral with respect to the technologies that can be used for IBA,[30] NAI members have historically used HTTP cookies for this purpose. However, member companies may also use non-cookie technologies for IBA purposes, so long as they do so in compliance with the Code, including provisions of requisite notice and choice (§ II.C.3.).




During the 2014 annual compliance review, NAI staff learned that many evaluated member companies were researching the use of other technologies for IBA and ADR. Many of these evaluated member companies indicated that they were awaiting further guidance from the NAI in order to use other technologies beyond cookies in a manner consistent with the Code. As a result, the NAI worked with its members in 2015 to develop and publish Guidance on the Use of Non-Cookie Technologies for Interest-Based Advertising.[31] This guidance clarifies how Code requirements may be met when member companies use non-cookie technologies for IBA and ADR.

More specifically, this guidance articulates the NAI's requirements for transparency, notice, control and accountability when member companies use non-cookie technologies. To illustrate, such companies must add to their privacy disclosures a statement that non-cookie technologies are being used for IBA and/or ADR. Furthermore, member companies must work with website publishers to include these disclosures in line with the NAI's pass-on notice requirements. To aid member companies, this guidance includes

30 *See Introduction and Commentary to Code.*

31 *See Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI Code of Conduct*, NAI (May 18, 2015), *available at* www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf.

In 2015 the NAI released its Guidance on Non-Cookie Technologies.

examples of language that can be passed on to website publishers. Additionally, member companies that use non-cookie technologies must increase transparency around their use of these technologies. To help facilitate this transparency, the NAI has developed, and is currently testing, a new consumer opt-out page that allows member companies to provide notice of their use of non-cookie technologies and to provide consumers a more robust choice mechanism when non-cookie technologies are used.

NAI staff continued to work with evaluated member companies to update their privacy disclosures to reflect the use of these additional technologies in those instances where evaluated member companies notified the NAI regarding such use (Code § II.A.1.d.).

Expanded technical reviews resulted in data collection reports, which provided aggregated summaries of members' data collection activities not easily visible using standard browser tools. Supplemented by the compliance questionnaires and telephone interviews, NAI staff endeavored to independently confirm when non-cookie technologies were used by evaluated member companies.[32] The NAI's data collection reports helped staff review 23,293 data elements, including cookies, URL queries, headers, Javascript files, pixel tags, and various markup languages—nearly 50 times more than last year. In several cases, these reviews helped spur discussions with members regarding their testing of non-cookie technologies.

The 2015 compliance review process and the NAI's technical reviews indicate that those members using non-cookie technologies for IBA or ADR are doing so in a manner consistent with the Code and with the Guidance on the Use of Non-Cookie Technologies for Interest-Based Advertising, by providing the required notice, transparency, and control under the Guidance.[33]

During the past year, public allegations surfaced regarding an evaluated member company using non-cookie technologies for IBA purposes without providing adequate levels of notice and control to consumers. Following an extensive investigation, the NAI Board of Directors determined that any alleged use of non-cookie technologies by the member company was not subject to NAI Code requirements, because at the time of this occurrence the enforcement of the Code was limited to the collection and use of data for IBA on desktop web browsers. The NAI Board of Directors determined that the alleged activity was limited to mobile devices only, and was not subject to NAI enforcement efforts at that time.[34] As of 2016, the NAI now fully enforces its Code as it applies to members' activities in mobile web browsers, and the App Code as it applies to members' activities in mobile applications.

32 The data collection report is produced by intercepting web packets from test browsers or devices and then creating an aggregate report of 30 supported data elements, including cookies, custom header fields, JavaScript functions, image metadata, and mobile data collection methods. Together, this helps reveal clues that a member is using an active statistical identifier or client-side storage.

33 The NAI is currently in an implementation period for this Guidance. This guidance is subject to change based on what is learned during the implementation period. During this implementation period, the NAI is evaluating the guidance and members' ability to comply with these requirements.

34 *See* discussion of the timeline of the NAI's enforcement efforts on mobile devices in the section of this Report titled 2015: A Year in Review.

# OPT-IN CONSENT

## Merger

During the 2015 annual compliance review evaluated member companies reported that they did not merge PII with Non-PII for IBA purposes. Accordingly, no evaluated member company sought to obtain consent for such merger.[35]

### The Code requires member companies to obtain Opt-In Consent for:

- the merger of PII with previously collected Non-PII for IBA purposes (§ II.C.1.c.);
- the use of "Precise Location Data" for IBA (§ II.C.1.d.);
- the use of "Sensitive Data" for IBA (§ II.C.1.e.); and
- for members who make a material change to their IBA data collection and use policies and practices (§ II.D.3.)

## Precise Location Data

The definition of "Precise Location Data" covers data obtained through a range of technologies, available either now or in the future, which may be able to provide "with reasonable specificity" the actual physical location of an individual or device (Code § I.G.) This definition of Precise Location Data excludes more general types of location data, such as postal zip code or city.

To help NAI members navigate the requirements for the use of these data points the NAI released guidance on Determining Whether Location is Imprecise.[36] This guidance is intended to help NAI members determine if the data they are using for IBA must be accompanied by Opt-In Consent, and encourages members to render location data imprecise before storage, by eliminating data points or truncating decimal points from coordinates. This guidance document suggests four factors that member companies should take into account when determining whether location data is imprecise, including the area of the identified location the population density of that area, the accuracy of the data, and the precision of the location data's timestamp. Ultimately the goal of this guidance is to protect consumer privacy, by providing a disincentive for the storage of data that could be used to determine the actual physical location of a device, while allowing for the use of broader location-based data, such as whether consumers are likely to visit coffee shops, or sit-down restaurants.

35 Member companies are also required to provide an Opt-Out Mechanism accompanied by robust notice for the use of PII to be merged with Non-PII on a going-forward basis for IBA purposes (prospective merger) (Code § II.C.1.b.).

36 *See Guidance for NAI Members: Determining Whether Location is Imprecise*, NAI (July 20, 2015), *available at* www.networkadvertising.org/sites/default/files/NAI_ImpreciseLocation.pdf.

NAI staff found during the 2015 annual compliance review that one evaluated member company was using Precise Location Data for IBA on desktop browsers. The evaluated member company attested to NAI staff that it sought to obtain Opt-In Consent for the use of the Precise Location Data for IBA through its publishing partners. (Code § II.C.1.d.). As the demand grows among advertisers for the use of Precise Location Data, and as the NAI begins enforcement of its App Code in 2016, the NAI plans to work with members to develop further guidance regarding the requirements for valid Opt-In Consent for this type of data collection and use.

## Sensitive Data

The NAI updated the term Sensitive Data in 2015. Sensitive Data is now defined to include specific types of PII that are sensitive in nature, as well as certain Non-PII related to health information and sexual orientation (Code § I.H.). NAI staff found that evaluated member companies did not use Sensitive Data for IBA purposes in 2015 and continued to have a uniformly high awareness of the requirements for the use of Sensitive Data for IBA. Consequently, evaluated member companies maintained the protections they had in place to ensure that Sensitive Data was not used for IBA.

The Code prohibits the delivery of IBA advertisements to users based on an inferred interest in sensitive health conditions, or based on actual knowledge about any health condition, without a user's Opt-In Consent. However, the NAI acknowledges that it is often difficult to draw bright lines between "sensitive" and "non-sensitive" data in the health space because whether a particular condition is considered sensitive may depend on the affected individual and a number of subjective considerations. Therefore, per the commentary to the Code, which outlines how the NAI will approach such issues, the NAI urged its evaluated member companies to conduct a reasonable analysis of health conditions and determine whether, based on an analysis of all the factors, those conditions should be considered to be sensitive.

During the annual compliance review, the NAI urged a few evaluated member companies to reconsider their use of certain segments involving health conditions that NAI staff determined were not Sensitive Data per se, but came close to meeting some of the criteria and factors outlined in the commentary to the Code.

Further, from the inception of the Privacy Disclosure Scanner, NAI staff was able to regularly review changes to the health segments publicly disclosed by most evaluated member companies, as required by the health transparency requirement of the Code. This enabled staff to work with members to help determine if a member added a segment that could be deemed sensitive per the analysis of relevant factors set forth in the commentary of the Code.

## In 2015 the NAI updated the definition of Sensitive Data.

The NAI received one complaint from an industry partner, alleging that an evaluated member company had targeted ads without obtaining Opt-In Consent featuring treatments for a sensitive mental health condition. The ads also included enhanced notice in the form of the industry icon. NAI staff investigated this complaint and held an extended interview with the evaluated member company in question. The member company clarified that its ads on the website in question were not targeted to specific individuals, and thus did not involve IBA or Retargeting, but rather were contextually determined based on the overall popularity of searches on that site. Contextual ads do not involve IBA or Retargeting. In other words, the ad was not targeted based on a browser's prior activity. NAI staff confirmed this assertion by visiting the website in question with a number of browsers, including clear browsers with no historical data, which all resulted in the same advertisements. The company used enhanced notice in all of its ads, whether they employed IBA or not, as a precaution.

In another instance, NAI staff noted during the annual review of one evaluated member company, that several segments, disclosed by the member in compliance with the NAI's health transparency requirement, would have required Opt-In Consent, which the company did not obtain. However, during further investigation by NAI staff, it became apparent that the member company misunderstood the transparency requirement, and had listed health conditions even when no associated data was retained for use in IBA or Retargeting.

The evaluated member company attested that it did not use information about the health conditions in question for IBA or Retargeting. NAI staff consequently found that the member company's practices were not subject to Code requirements for Opt-In Consent or health transparency.

### Sexual Orientation

The Code prohibits member companies from using data collected across unaffiliated web domains to associate a browser or device with IBA segments or categories that presume or infer an interest in gay, lesbian, bisexual, or transgender information, products, or services without obtaining Opt-In Consent. NAI members recognize that LGBT status may be considered sensitive in some contexts, and thus that Opt-In Consent should be obtained before using such data for IBA. Through the compliance review process, NAI staff found that no evaluated member companies created or used LGBT audience segments for IBA.

The effectiveness and reach of this provision was manifested when advertisers of products and services aimed at the LGBT community reached out to NAI staff to discuss this NAI requirement, and to discuss potential methods for obtaining Opt-In Consent, allowing them to work with NAI member companies while utilizing IBA and Retargeting to find their audiences.

### Material Change

The Code requires that members who make a material change to their IBA data collection and use policies and practices obtain Opt-In Consent before applying such change to data collected prior to the change (§ II.D.3.). In 2015 NAI staff questioned evaluated member companies and discussed their business models to help identify any potential material change relating to their policies and practices regarding IBA, and evaluated member companies attested their compliance with this provision.

## PERSONALLY IDENTIFIABLE INFORMATION (PII)

The Code encourages data minimization by placing greater restrictions on the use of PII for IBA.[37] Most significantly, the Code requires heightened notice and choice for the use of PII for IBA purposes. As a result of the disincentives imposed by the Code for the use PII for IBA purposes, in 2015 NAI staff found that not one of the evaluated member companies used PII for IBA purposes.

Evaluated member companies, in fact, continued to employ mechanisms to help ensure that they did not inadvertently collect or receive PII for IBA purposes. They often imposed contractual restrictions forbidding their data providers or partners from passing PII to them, and some reinforced these contractual requirements through technical controls that immediately discarded PII unintentionally passed to the member company for IBA purposes.

37 The Code also provides that members contractually require any unaffiliated parties to which they provide PII for IBA or ADR services to adhere to applicable provisions of the Code (§ II.E.1); obligates members to contractually require that all parties to whom they provide Non-PII collected across web domains owned or operated by different entities not attempt to merge such Non-PII with PII held by the receiving party or to re-identify the individual without obtaining the individual's Opt-In Consent (this requirement does not apply where the Non-PII is proprietary data of the receiving party) (§ II.E.2); and requires members to provide consumers with reasonable access to PII and other information associated with that PII retained by the member for IBA (§ II.F.1.).

# USE LIMITATIONS

## Children

The Code requires that members obtain verifiable parental consent for the creation of IBA segments specifically targeting children under 13 years of age (§ II.D.1.). During the 2015 annual review, all evaluated member companies indicated awareness of the sensitivity of data related to children for IBA, and advised the NAI that they had processes, policies, and procedures in place to prevent creation of IBA segments specifically targeted at children under 13.[38]

## Eligibility

All evaluated member companies affirmed during their annual compliance reviews that they do not use, or allow the use of, data collected for IBA or ADR for the purpose of determining or making the following eligibility decisions: employment; credit; health care; insurance, including underwriting and pricing, as forbidden by the Code (§ II.D.2.).

Aside from the expressly forbidden eligibility uses of IBA and ADR data detailed above, in 2015 NAI staff also used the compliance reviews as an opportunity to educate its members about the need to avoid other potentially problematic uses of IBA and ADR data, such as for tenancy or education admissions eligibility. Based on NAI staff discussions with evaluated member companies it appears that members did not use, and were not aware of any partner use of, IBA and ADR data for these purposes.

## Transfer Restrictions

During the 2015 annual compliance review, evaluated member companies attested that they were in compliance with the obligation to contractually require any partners to whom they provide Non-PII, to be merged with PII data possessed by that partner for IBA, to adhere to the applicable provisions of the (Code § II.E.1.).

Evaluated member companies further attested that they complied with the requirement that they contractually require that all parties to whom they provide Non-PII, collected across web domains owned or operated by different entities, to not attempt to merge such data with PII held by the receiving party or to re-identify the individual for IBA purposes without obtaining Opt-In Consent (Code § II.E.2.).

38 Independently of NAI Code requirements, member companies are, of course, expected to abide by the laws applicable to their businesses.

# DATA ACCESS, QUALITY, SECURITY, AND RETENTION

## Reasonable Access to PII

As discussed, the NAI staff confirmed with evaluated member companies that they did not collect PII for IBA purposes. Accordingly, it was not necessary for NAI staff to evaluate access requirements to PII[39] (as required by the Code) in 2015.

## Reliable Sources

Evaluated member companies once more attested, and explained in interviews, that they obtain data from reliable sources (Code § II.F.2.). Evaluated member companies overwhelmingly reported conducting appropriate due diligence on data sources to help ensure their reliability, including reviewing the potential partners' business practices, particularly when those partners were not members of the NAI and thus could not be counted on to have undergone the same compliance review. NAI staff continued to offer suggestions and best practices to evaluated member companies to help them develop even more due diligence processes in regard to data partners.

## Reasonable Security

The Code imposes a requirement designed to help ensure that data used for IBA activities is adequately secured. Evaluated member companies attested that they were in compliance with the obligation to reasonably secure data collected for IBA and ADR. (Code § II.F.3.).[40]

39 Code § II.F.1. requires members to provide users with reasonable access to PII (such as name or email address) used for IBA, but does not require members to provide consumer access to strictly Non-PII data such as interest segments tied to cookies or other Non-PII identifiers.

40 During the annual compliance review, evaluated member companies are required to attest in writing that they have reasonable and appropriate procedures in place to secure their data as required by the Code. However, as with past compliance reviews, NAI staff did not conduct security audits of evaluated member companies or otherwise review their data security practices. NAI staff did not advise evaluated member companies on specific data security measures, as what is reasonable and appropriate depends on the evaluated member companies' business models. Because business models vary, member companies, not NAI staff, are in the better position to determine what is appropriate under a given set of circumstances.

### Retention

During the 2015 annual compliance review, NAI staff discussed with evaluated member companies the Code requirement to retain data only as long as necessary for a legitimate business purpose (§ II.F.4.). Evaluated member companies were required to attest to the longest duration of IBA data storage on their servers. In accordance with section II.B.1.f., member companies are also required to publicly disclose the period for which they retain such data for those purposes.

NAI staff continued to manually examine the expiration dates of evaluated member companies' cookies and posed additional questions when those cookies' lifespans exceeded the stated retention period. NAI staff then confirmed that evaluated member companies' privacy disclosures clearly and conspicuously explained these retention practices. As in the past, NAI staff utilized these compliance reviews to encourage evaluated member companies to further reduce their data retention periods, while highlighting the need for data minimization in general. Several companies indicated that they are exploring shorter data retention periods.

## ACCOUNTABILITY

To help ensure compliance with the Code, each evaluated member company has designated at least one individual with responsibility for managing the member's compliance and providing training to relevant staff within the company. (Code § III.A.2.) Further, evaluated member companies overwhelmingly met the requirement to publicly disclose their membership in the NAI and compliance with the Code. The few evaluated member companies that were unclear in their public disclosure of NAI membership and adherence to the NAI Code worked with NAI staff to improve these disclosures (Code § III.A.3.).

## SANCTIONS

A thorough compliance assessment process and the availability of strong sanctions combine to form the keystone of the NAI self-regulatory program. NAI staff investigates private and public allegations of noncompliance. Staff also searches for evidence of noncompliance in the reports generated by the NAI's automated monitoring tools. In the event that NAI staff finds, during any of the compliance processes, that a member company may have materially violated the Code, the matter may be referred to the Compliance Committee of the Board of Directors with a recommendation for sanctions.[41] Should the NAI Board determine that a member has materially violated the Code, the NAI may impose sanctions, including suspension or revocation of membership. The NAI may ultimately refer the matter to the FTC if a member company refuses to comply. The NAI may also publicly name a company in this compliance report, and/or elsewhere as needed, when the NAI determines that the member engaged in a material violation of the Code.

In 2015 NAI staff conducted several investigations of potential material violations of the Code. Ultimately NAI staff or the NAI Board of Directors found that the member companies in question either did not violate the Code or that the alleged activities fell outside the scope of the NAI's enforcement efforts, and consequently, sanctions procedures were not appropriate.

In 2015 NAI staff found a number of lesser, nonmaterial potential violations of the Code by some member companies. Throughout the year, these member companies willingly resolved such issues raised by NAI staff, frequently implementing additional measures voluntarily to guard against future noncompliance. Based on its historical approach to minor infractions, typically caused by misunderstandings or technical glitches, NAI staff worked with members to resolve issues before they become material violations of the Code. This approach helped fix issues expeditiously, while reserving sanctions for material Code violations, and helping to ensure the vitality of the ecosystem.

The NAI continues to strongly believe that by identifying problems early, and giving member companies an opportunity to resolve minor transgressions, any potential issues are addressed before they can affect the broader population and therefore become material, thus necessitating stronger sanctions. This approach fosters an environment of mutual trust between the NAI and its members, and ultimately results in more privacy protection for consumers as members become more open about potential shortcomings and more willing to work on solutions.

## SUMMARY OF FINDINGS

NAI staff found that in 2015 evaluated member companies overwhelmingly complied with the Code, and to the extent that any violations were identified, they were not material. Evaluated member companies demonstrated that they remain vigorously committed to the NAI's self-regulatory framework. Representatives from evaluated member companies welcomed feedback and best-practice suggestions from NAI staff, and appeared to be genuinely concerned with providing top-notch privacy protection programs.

41 *See NAI Compliance and Enforcement Procedures*, NAI, *available at* www.networkadvertising.org/pdfs/NAI_Compliance_and_Enforcement%20Procedures.pdf (for further details about the NAI enforcement procedures).

# CONCLUSION

This report demonstrates that the NAI plays an increasingly important role in promoting consumer privacy in the online advertising technology ecosystem, while working to keep informed of industry developments and to provide up-to-date guidance to its member companies. Throughout 2015 the NAI released updated versions of the Code and the App Code, as well as two important guidance documents, while continuing to work with a variety of stakeholders on other initiatives that may come to fruition in 2016 or beyond. During this time the NAI also further developed its monitoring capabilities, and by extension, its ability to identify and minimize events with a potentially negative impact on consumer privacy. This report also establishes that through its annual compliance review process, the NAI and its staff maintain a close connection with the ecosystem, identifying industry trends as well as associated problems and opportunities for improvement. The review process manifests NAI member companies' determination to protect consumer privacy. These companies form a core of responsible actors in the ecosystem, through a commitment to some of the strongest self-regulatory principles in the industry.

The NAI is satisfied with the results of its annual compliance review, and the efforts of its members to comply with the Code and other NAI guidance. However, there is always room for improvement, and in 2016 the NAI plans to further enhance its consumer education materials, including more information on new technologies and data collection across mobile applications. The NAI also plans to work on synthesizing its Code and App Code into one document in order to make NAI requirements easier to grasp for the public, and to streamline compliance efforts for NAI members. The NAI will also continue to work with its members and with industry stakeholders as it further explores a role for potential guidance regarding cross-device applications in online advertising.

On a technical front, the NAI will advance its resources by pursuing further enhanced monitoring capabilities focused on data collection across mobile applications and other cookie-less technologies. These developments will coincide with the planned public launch of the revamped NAI opt-out page, enabling consumers to verify when NAI members are collecting and using data for IBA with non-cookie technologies, and facilitating consumer choice when non-cookie technologies are used for IBA.

As NAI members continue to face the privacy challenges of emerging technologies and business lines, the NAI is able to leverage its unique position in the advertising technology ecosystem to monitor companies' compliance, and where to next focus NAI resources in years to come. In particular, the NAI is able to use its members' and staff expertise and know-how to apply effectively existing privacy standards to new technologies. The NAI believes that it will take an industry-wide effort to balance the privacy needs of consumers with the technological advances that accompany the introduction of new data collection methods.

Washington Office
509 7th Street, NW
Washington, DC 20004
www.networkadvertising.org

NAI
Network Advertising Initiative