I am proud to present the Network Advertising Initiative's (NAI) 2014 Annual Compliance Report. The Report provides a summary of members’ adherence to the NAI Code of Conduct based on findings from the NAI staff’s ongoing monitoring processes during the 2014 compliance period.

NAI is set apart in our industry by its high standards for Interest-Based Advertising and related business models applicable to its third-party advertising members. For the past seven years, I have worked with NAI in two different capacities: first, serving as a Board Member representing a member company and now as NAI General Counsel and VP for Compliance and Policy. These two different vantage points have enabled me to obtain unique insight into the organization’s tremendous efforts in ensuring that NAI’s Self-Regulatory Code of Conduct continues to lead our industry forward at this critical time.

Setting high standards that embody the Fair Information Practice Principles of notice, choice, use limitations, data security, access, and accountability is just one part of NAI’s important role. The other part focuses on the last principle – accountability. Accountability is at the heart of what we do at NAI and why NAI maintains a comprehensive program to ensure compliance with these standards. We know that even the highest standards for self-regulation are meaningless without a rigorous enforcement process and an insistence on accountability.

The compliance staff and I are responsible for monitoring and enforcing the Code and then publishing NAI’s Annual Compliance Report. The report provides a summary of NAI staffs’ findings from its monitoring processes during the 2014 compliance period (January 1 to December 31, 2014). This includes investigations and enforcement proceedings conducted during that time period. NAI is committed to transparency, and publishing the report allows consumers, members, regulators and other interested parties to evaluate the compliance program and self-regulatory process for themselves.

It is worth noting that the compliance process begins before NAI members even join our organization. NAI staff conducts a thorough review of every applicant before any company can claim NAI membership.

NAI staff then continues helping members with their ongoing compliance maintenance by staying in ongoing contact with them, providing educational webinars about the Code, and discussing specific Code provisions with members on a one-to-one basis. NAI also uses unique technical monitoring tools developed by NAI staff for compliance purposes. For example, NAI compliance technology monitors our members’ opt-out mechanisms and regularly gathers data on their functionality and reliability. In 2014, NAI began using a scanner that alerts NAI staff to changes to members’ privacy policies. The privacy disclosure tool provides reports to the NAI compliance staff if a member company revises its privacy policy. We then review the reports so that we can be alerted to any possible changes or deletions which may drop required Code notices.
These processes allow NAI staff to identify potential Code violations and work with members to quickly address issues before they affect a large number of consumers. However, we won’t rest on our laurels – NAI will be working throughout 2015 to update these tools and monitoring processes in an ongoing effort to make our program even stronger.

The Annual Compliance Report is a summary of the results of the aforementioned compliance efforts as well as comprehensive annual reviews with member companies. None of the issues discovered by NAI staff in the 2014 compliance period were deemed to constitute 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. In addition, many members went on to develop and provide technical and administrative checks to help prevent similar issues from recurring as well as provide training to employees to flag and respond to such issues.

This is a critical point. NAI staff may identify numerous potential issues over the course of the year. In fact, through its technical monitoring tools, during the 2014 compliance period, NAI identified about 20 broken opt outs on the NAI site or missing Code required disclosures in privacy policies. Members rapidly resolved these issues. NAI did not sanction, nor did it name in this annual compliance report, members for immaterial violations of the Code. Our members know that they can interact with us openly and honestly to fix problems. We believe that this leads to a stronger compliance program. To be clear, NAI retains the option to sanction members if Code violations are found to be material; however, we have found that maintaining dialogue and communication with member companies on an ongoing basis helps resolve issues quickly to the benefit of the consumer and increases the overall health of the ecosystem.

As demonstrated through this report, industry can and does effectively regulate itself. Even in the face of increasing uncertainty in the marketplace and new competitive challenges, NAI members overwhelmingly met their obligations and demonstrated their commitment to consumer privacy and industry best practices.

Noga Rosenthal
General Counsel, VP for Compliance and Policy
For the past 15 years, the Network Advertising Initiative (NAI) has been the leading nonprofit self-regulatory trade association governing technology companies engaged in digital advertising. It is a membership-based organization comprised of third-party digital advertising companies.
NAI is the leading self-regulatory trade association governing third party technology companies engaged in digital advertising.

NAI first developed and adopted a set of self-regulatory policies for online advertising, the Self-Regulatory Principles, in 2000. At the time, in its Report on Online Profiling, the Federal Trade Commission (FTC) “unanimously applaud[ed]” NAI for developing these groundbreaking principles. NAI updated its self-regulatory principles, also referred to as the Code of Conduct (Code), twice, in 2008 and 2013. The Fair Information Practice Principles (FIPPs) have notably served as the underlying basis for every iteration of the Code. The Code applies FIPPs to the Interest-Based Advertising (IBA) and Ad Delivery and Reporting (ADR) activities of member companies in the United States.

Overall, the goal of the Code is to incentivize privacy by design and responsible data collection and use practices by NAI members. For example, Code requirements often lead members to implement layered administrative, technical and physical controls when building their databases to prevent the unintentional collection and/or collection of Personally Identifiable Information (PII) for IBA activities. Further, the Code requires that members set retention schedules for their data. Members can then build their systems with the retention period in mind, promoting data minimization and the timely deletion or de-identification of data. Members are further required to provide consumers with notice and choice around members’ IBA practices. This includes a disclosure describing the member’s IBA activities. Additionally, the Code limits the uses of data collected for IBA and restricts certain transfers of such data to third parties. It also requires members to work with “reliable” data sources and to secure the data they collect for IBA.
In order to provide an effective self-regulatory framework, the Code is backed by rigorous compliance and enforcement procedures. Compliance, more fully discussed below, includes the following:

- **On-Boarding Process:** NAI staff conducts detailed evaluations of applicants’ business models prior to their admission to NAI to help confirm that their business practices are capable of meeting the requirements of the Code.

- **Technical Monitoring:** 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:** 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:** NAI evaluates allegations of non-compliance with the Code from other sources, such as regulators, competitors and privacy advocates.

- **Annual Compliance Reviews:** 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 – even as their business models evolve.

- **Enforcement:** NAI members are subject to formal sanctions for material non-compliance with the Code.

- **Publication of the Annual Compliance Report:** NAI provides consumers, regulators and others visibility into NAI’s compliance program and self-regulatory process through publication of this annual compliance report.
Through the 2014 compliance review process, NAI found that member companies are overwhelmingly meeting the requirements of the 2013 Code of Conduct:

<table>
<thead>
<tr>
<th>Education (§ I.A.)</th>
<th>Use Limitations (§ I.D.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 2014, members donated 5.5 billion impressions to NAI’s education campaign, tripling the number of donations from members in 2013. The NAI campaign helped educate consumers about IBA and consumer choice, helping to lead to over 4.5 million page views on NAI education pages in 2014 – over 1.5 million more visits than in 2013.</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transparency and Notice (§ I.B.)</th>
<th>Transfer Restrictions (§ I.E.)</th>
</tr>
</thead>
</table>
| Members continued to provide consumer-facing notices about their data collection and use practices for IBA and ADR.  
  - First, members provided notice in their privacy disclosures on their own sites regarding their IBA and ADR activities.  
  - 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.  
  Member companies also provided notice and choice in or around advertisements through an enhanced notice mechanism.  
  Finally, members worked to disclose the standard health segments they used for IBA. | 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 without Opt-In Consent where Non-PII is not proprietary to the receiving party. |

<table>
<thead>
<tr>
<th>User Control (§ I.C.)</th>
<th>Data Access, Quality, Security &amp; Retention (§ I.F.)</th>
</tr>
</thead>
</table>
| All NAI members offered links to Opt-Out Mechanisms from their own sites. There were upwards of 5 million visits to NAI opt-out page in 2014- over a million more visits than in 2013.  
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. Members also diligently monitored the Opt-Out Mechanisms on their own sites. | 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. |
While NAI staff found members to be overwhelmingly in compliance with the Code, and confirmed that members took proactive steps to ensure that they remained in compliance with the Code, NAI staff found minor issues throughout the compliance period. For example, the NAI’s technical monitoring and compliance reviews helped discover minor problems with opt out functionality or with disclosures required by the Code. NAI staff identified approximately 20 broken opt outs on the NAI site and required disclosures missing in privacy policies. Members quickly fixed their opt out problems once NAI staff contacted them. NAI’s monitoring tool also caught inadvertent deletions of a notice provision required by the Code or a broken privacy policy link or opt out link within privacy disclosures – which members quickly reinserted upon notice from NAI staff. Again, in all such similar cases, NAI staff worked with members to rectify any issues in a prompt manner before these minor potential infractions could turn into larger matters affecting a large number of consumers. NAI’s own independent testing found other issues. For instance, NAI staff discovered that several members’ email links were broken when testing members’ mechanisms to answer consumer inquiries. Members quickly fixed the broken links once the matter was brought to their attention.

NAI staff also worked with members through 2014 to answer their questions prior to launching a new product or service. NAI staff conducted about 25 investigations and reviews into such matters including the use of new technologies on desktop and mobile browsers for IBA and/or ADR, the use of various health segments for IBA and the integration of two NAI member companies. These assessments enabled NAI staff to highlight potential issues to members, such as the technical ramifications of merging two NAI member companies’ opt out mechanisms.

Additionally NAI staff conducted a number of investigations regarding potential non-compliance with the Code. NAI staff then consulted the NAI Board Compliance Committee on several such matters. In all such cases, reviewed between January 1st, to December 31st, 2014, NAI staff either did not find a violation of the Code or found that the violations were non-material because they were inadvertent and affected a very limited amount of users before being rectified. This reflects NAI’s longstanding policy of maintaining 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.
NAI brings sanctions against a member when appropriate, such as when a member willingly or materially violates the Code or does not cooperate with NAI staff. This approach of working with members to help fix problems expeditiously, while reserving sanctions for material Code violation, helps to ensure the health of the ecosystem. Most importantly, it helps to preserve consumer privacy by ensuring that member companies continue to subject themselves to self-regulation, and maintain an open dialog between member companies and NAI staff in which members can discuss their business practices and policies without fear that every minor infraction will become publicized. Ultimately, the goal of NAI’s compliance program is to ensure that as many companies as possible provide consumers with the privacy protections required by the NAI Code, rather than to embarrass members by revealing every potential glitch or mistake they may make.
INTRODUCTION

For fifteen years, the not-for-profit Network Advertising Initiative (NAI) has been the 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.\(^3\) Members include a wide range of businesses such as ad networks, exchanges, platforms,\(^4\) data aggregators, and other technology providers. At the time of publication, NAI has 96 members. These intermediaries play a pivotal role in the digital advertising ecosystem – linking advertisers and trusted brands with those consumers most likely to be interested in their products and services. This relevant advertising, in turn, helps power free content and services in the digital ecosystem.\(^5\)

---

1 IBA is defined in the Code to mean “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 Code imposes requirements with respect to “Ad Delivery & Reporting,” which are separate and distinct activities from IBA. ADR is defined in the Code 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.” Ad Delivery and Reporting (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 (Code § I.B.).

3 The Code covers activities that occur 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 and ADR activities for the purposes of this compliance report.

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

Member companies work together to guide NAI in setting proper guidelines around data collection and use. The goal of NAI and its members is to maintain consumer trust while providing a relevant digital advertising experience. NAI helps its members foster this trust through a comprehensive self-regulatory program that includes a Code of Conduct backed by robust compliance and ongoing enforcement.

This report provides a summary of the NAI staff’s findings from the 2014 compliance period. During the 2014 compliance period, NAI staff reviewed members’ compliance with the 2013 Code of Conduct, which went into enforcement as of January 1, 2014. Through publication of this report, consumers, regulators and others gain visibility into NAI’s compliance program and self-regulatory process. In addition, this report helps illustrate how the compliance process shapes the evolution of NAI’s policies and procedures, including goals for further improvement of the compliance program in 2015.

---

6 This report addresses the compliance process from January 1st, to December 31, 2014, including any investigations of material violations of the Code or enforcement proceedings conducted during that time period.

ON-BOARDING NEW MEMBERS - COMPLIANCE BEGINS EVEN BEFORE COMPANIES JOIN

Companies can’t simply join NAI; they must commit to compliance. Compliance begins with the on-boarding process. NAI staff first prescreen potential applicants to ensure that their business models fit within the Code. At least two attorneys on the NAI staff evaluate each applicant’s business model and privacy practices. Specifically, NAI staff reviews a company’s application questionnaire, privacy disclosures, and choice mechanisms for data collection, use, retention, and sharing practices to ensure they are consistent with the Code. Then, NAI staff conducts an interview with high-level staff at the applicant company wherein the applicant is subject to further questions regarding discrepancies, if any, in their application materials, or business practices that may be inconsistent with the Code.

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 highlights those that need to be addressed before it can become a member of NAI. Often, this assessment can be a months-long process, with NAI providing guidance and suggestions about Code compliance at every step. Most applicants make substantial revisions to their public privacy notices and disclosures in order to provide the full level of notice required by the Code. Typically, NAI staff provide technical guidance to help an applicant develop a fully functional
Companies can’t simply join NAI; they must commit to compliance.

Opt-Out Mechanism⁸ that can both meet the Code’s requirements and be compatible with the NAI opt-out page. On occasion, applicants have abandoned existing or planned 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 full NAI Board of Directors. The NAI Board of Directors is comprised of seasoned attorneys and compliance executives from 12 leading companies. The Board reviews each application, often requesting additional information from an applicant, before voting to accept a new member. Therefore, each potential member is reviewed by both the 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 NAI.

In 2014, five companies⁹ completed the on-boarding process and were approved for membership by the Board.

2014 NAI Board Members:

Alan Chapell, President of Chapell and Associates, representing Audience Science
Alexis Goltra, Chief Privacy Officer and Asst. General Counsel for Privacy & Security, Oracle
Andrew Pancer, Chief Operating Officer, Distillery
Brooks Dobbs, Chief Privacy Officer, KBMGroup
David Wainberg, 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 (formerly, 24/7 Media)
Michael Benedek, President and CEO, Datonics
Shane Wiley, Vice President of Privacy & Data Governance, Yahoo!
Ted Lazarus, Director, Legal, Google

---

⁸ Opt-Out Mechanism is defined under the Code as “an easy-to-use mechanism by which users may exercise choice to disallow Interest-Based Advertising with respect to a particular browser or device” (Code § I.I.).

⁹ The following went through the pre-certification process and became NAI members in 2014:
1. Run, Inc. 2. GumGum, Inc. 3. Tapad, Inc. 4. Simplifi Holdings, Inc. 5. Varick Media Management.
MONITORING OF MEMBERS

NAI Technical Monitoring

NAI continues helping members with compliance with the Code through its technical monitoring tools. Currently, NAI has two tools that help members ensure that they remain compliant with the Code between annual compliance reviews: an “Opt-Out Scanner” and a “Privacy Disclosures Scanner.” The Opt-Out Scanner generates a report on potential technical issues around a member’s opt-out cookies. The Privacy Disclosures Scanner, which was launched in 2014, creates reports that NAI staff review to note changes to members’ privacy disclosures. Changes may include revisions to, or the accidental deletion of, disclosure language that may be required by the Code. One of the main benefits of NAI’s technical monitoring tools is their ability to help NAI staff spot potential Code violations quickly, enabling NAI to address concerns with members prior to these affecting large numbers of consumers.

Opt-Out Scanner

The Opt-Out Scanner uses automated Web crawls of over 200 ad-heavy web pages to gather data related to the member’s opt-out functionality and reliability. It analyzes the crawl data for signs of potential issues and then produces aggregate reports of these analyses to NAI staff.

Throughout 2014, NAI staff reviewed these reports to identify and address potential problems with member Opt-Out Mechanisms. Specifically, the Opt-Out Scanner is designed to detect if an opt out failed to properly set the correct cookies on the NAI opt-out page, if an opt-out cookie was removed or modified during the crawl, and/or if any potential IBA cookies were set while an opt-out is present on a browser. These issues can be the result of incomplete server migrations and potential bugs in new products and services.

In 2014, NAI introduced an in-house tool to scan over 275 pages of privacy disclosures of existing members’ and potential applicants’ for any changes made to those disclosures.

Working together, NAI and members sought to assure that any potential downtime of an opt-out was as minimal as possible. Every issue that was identified using the Opt-Out Scanner was resolved by members after being contacted by NAI. None of these issues were deemed to constitute material non-compliance with the Code because the underlying issue was resolved quickly, was found to be unintentional and affected a limited number of consumers. In addition, many members experiencing technical problems went on to develop and provide additional technical and administrative checks to help prevent similar issues from recurring.

10 Under the Code, each member is required to provide and honor consumer choice to disallow IBA data collection and use by a member on a particular browser through an Opt-Out Mechanism (§ II.C.2.). This requirement is discussed more fully below.
Privacy Disclosures Scanner

In 2014, NAI introduced an in-house tool to scan over 275 privacy policy disclosures of members and applicants for changes to those disclosures. The Privacy Disclosures Scanner checks web pages on a word-for-word basis for deletions and additions as well as errors in accessing those web pages. NAI began using the Privacy Disclosures Scanner in June 2014. The scanner was used over 120 times in 2014. The scans helped NAI staff identify a range of potential compliance issues, including privacy policy revisions and problems in accessing links in privacy disclosures or Opt-Out Mechanisms. NAI staff worked with members to ensure any issues identified using the Privacy Disclosures Scanner were fixed promptly.

In addition, the Privacy Disclosures Scanner helped bring numerous business model changes to the attention of NAI staff, such as new products and acquisitions. Because disclosures in privacy policies usually occur in anticipation of launching a new product, spotting these changes allowed NAI staff to help members evaluate how to configure their products or services with privacy in mind. For example, the Privacy Disclosure Scanner helps provide NAI staff early knowledge of a member’s potential use of non-cookie technologies, providing NAI staff the opportunity to work with the member to understand innovations in the marketplace and implications under the Code before these technologies are actually used in practice. Furthermore, knowledge of new business models that may have arisen in 2014 helped inform NAI’s monitoring tools and can help NAI staff incorporate new concepts into the 2015 annual compliance reviews.
Overall, the majority of the changes to members’ privacy disclosures were positive. Many changes were the result of members and applicants responding to action items and feedback provided by the NAI staff. Further, any deletions or changes of language required by the Code were deemed immaterial by NAI staff because they were reinserted or updated to comply with the Code within a reasonable time from NAI staff’s notice to the member. NAI staff acknowledges that members face the difficult task of explaining to consumers in a clear and meaningful manner through their privacy disclosures what data they are collecting and using for digital advertising. Members work hard to have accurate privacy policies. NAI recognizes that members must balance the need to be concise with the need to be transparent. NAI staff applies its knowledge of the industry, knowledge of the Code and expert judgment in determining the adequacy of disclosures in a member’s privacy disclosure from an NAI Code perspective.

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 2014, NAI received and reviewed almost 9,000 consumer queries through its website and several queries through physical mail. NAI staff determined that the majority of the inquiries pertained to issues outside of the scope of the NAI’s mission. For example, many emails asked questions about junk mail, spam, and pop-ups, which are not issues covered by the Code.¹¹

Most of the remaining consumer inquiries related to requests for assistance in troubleshooting technical issues with opt outs. NAI responded with guidance related to how to reset opt-outs 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 summary, NAI staff determined that in 2014, consumer communication received by the NAI through email, phone, letter or the website that were conducive to resolution had been resolved within a reasonable timeframe and were non-material. Therefore, no issues raised through consumer communications were escalated to the NAI Board.

Consumer Question Mechanisms

During 2014, NAI staff reviewed members’ sites and confirmed that they provided mechanisms on their websites through which consumers could submit questions or complaints directly to the member (§III.C.2.).

11 The Code does not require that the NAI members maintain opt-out programs for postal or electronic mail nor require that members provide unsubscribe mechanisms for emails, text messages, or for pop-ups. Instead, the opt-out tool covers NAI members’ IBA for advertising on desktop browsers based on users’ web browsing.
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 such member’s collection and use of data for IBA. NAI staff found that the overwhelming majority of members provided an email address or web-based form for consumers to use for questions. One member did not have a mechanism for a consumer to submit complaints or questions. Once the matter was brought to the member’s attention, the oversight was fixed in a timeframe that NAI staff deemed reasonable. Another member only provided a physical mailing address. NAI staff recommended that the member with only a physical mailing address change its practices to also include an email address to provide consumers an easier mechanism to send in their questions, even though providing a physical address for inquiries does comply with the Code.

In 2014, NAI staff also independently tested members’ responses to consumer questions about opting out of IBA. NAI sent test emails to member companies with questions asking how to opt out of IBA. Of the evaluated member companies offering an email address for questions, almost 85% responded promptly and with informative responses about their IBA activities.

In twelve instances, NAI staff found that the test email bounced back. Those member companies with a broken email link fixed the issue promptly after notice from NAI staff. NAI staff reminded these members of the need to have a functioning contact mechanism on their websites and to respond to any consumer questions or concerns in a proper manner.

The remaining members with issues around their consumer replies either completely failed to respond to consumer inquiries, did not respond in a prompt manner or did not respond to the consumer question about IBA properly. For instance, one company incorrectly told the consumer how to opt out of its corporate marketing emails, not IBA by the member. The member company did not ask what type of data collection and/or use the consumer wished to opt out of. NAI worked with the member company to devise a process to properly evaluate and respond to consumer questions.

After being contacted by NAI staff, other members reported that they quickly updated their processes for responding to consumer questions to ensure that consumer questions with respect to IBA practices are timely and accurately addressed. Due to this testing, one member initiated a training session for its employees in early 2015 to properly answer consumer inquiries around IBA and choice. Another member held an internal meeting with staff to once again emphasize the importance of properly

---

12 Further, during 2015, the Privacy Disclosure Scanner will enable the NAI staff to detect if a member’s email link is broken.
and promptly answering consumers’ questions around the member’s privacy policy and IBA. A third member immediately updated its standard response language to questions received through the email to describe consumer’s choice around IBA. NAI staff re-tested those affected members’ consumer communications mechanisms, and received a timely response from each providing information about IBA practices.

Investigating Other Complaints

Between January 1st and December 31st, of 2014, NAI staff investigated a number of instances of potential non-compliance with the Code. Some of these investigations resulted from NAI staff findings during the annual compliance review process, while others were instigated by public allegations about a company’s practices, or complaints to NAI by third parties.

These investigations included the use of non-cookie technologies, delivery of notice in and around targeted advertisements, opt-out status messaging, and uses of various data sources for IBA.

The investigations and reviews during this compliance period included the application of the Code to the alleged practices, discussions with relevant member companies and the review of public and non-public facts. In particular, these investigations looked into the amount of users potentially affected by the issues, the circumstances leading to the alleged problems, and the member companies’ actions to remediate the alleged problems. In all cases during this investigation period, NAI staff, or the NAI Board of Directors Compliance Committee, determined that the allegations either did not constitute a violation of the Code or did not rise to the level of a material violation of the Code, and therefore, sanctions procedures were not appropriate. In the event that remedial actions by the member company were required, these were performed swiftly, often within hours of a request by NAI staff.
ANNUAL REVIEW

The annual compliance review provides a snapshot of members’ business models, policies and practices and NAI staff’s efforts to help them confirm that members continue to comply with the Code even as individual businesses and the industry as a whole evolve. As the Code currently covers members’ IBA and ADR activities on desktop web activities only, NAI staff’s review was limited to desktop browsers. The application and enforcement of the NAI self-regulatory principles across mobile devices (including mobile web browsers and mobile applications) are scheduled to begin sometime in 2015. The Code will also govern members’ IBA and ADR activities across websites accessed from mobile devices at that time.

For the 2014 annual compliance review, NAI staff reviewed the 92 companies that were members prior to January 1, 2014. These members will be referred to as “evaluated member companies” throughout this report. Those members that joined NAI as of after January 1, 2014, were subject to review during the calendar year as part of the on-boarding process, and therefore were not part of the 2014 annual compliance review. They will be assessed again during the 2015 annual review process.

13 Certain practices, such as the provisioning of offline data for use in targeted online advertising, are not directly covered by this Code. Some member companies have committed to applying NAI principles to these practices in order to further promote consumer privacy. NAI enforces the relevant NAI Code provisions to such members. NAI will apply any future updates to the Code that cover provisioning of offline data for use in targeted advertising to all NAI members.

14 The following companies are no longer members of the NAI: a) Kontera Tech determined to leave the NAI in 2014. However, Kontera was evaluated by NAI staff during its 2014 annual compliance review. b) Core Audience represented to NAI staff that it is no longer engaged in IBA activities. It did not undergo the 2014 annual compliance review. c) Adapt.tv and Buysight were both absorbed by AOL and ceased to have independent operations, and therefore were not evaluated independently of AOL during the 2014 annual review process.

15 See supra, note 9.

16 NAI staff make an effort to review new member companies first, during the subsequent annual review, in order to minimize the time between a member’s initial on-boarding review and its first annual compliance review.

---

Evaluated Member Companies

- 33 Across
- Accuen
- Adara Media
- Adblade
- AddThis
- AdRoll
- Aggregate Knowledge
- AOL Advertising
- AppNexus
- Atlas Solutions
- Audience Science
- Batanga Network
- Bazaarvoice
- Bizo
- BlueKai
- Brightroll
- Brilig
- Burst Media Corporation
- Chango
- ChoiceStream
- Cognitive Match
- Collective
- Conversant (formerly ValueClick, MediaLink, and Dotomi)
- Criteo
- Cross Pixel
- DataLogix
- DataXu
- Datonics
- Defy Media (formerly Break Media)
- Distillery
- eBay Enterprise (formerly Fetchback)
- eXelate
- Exponential Interactive (formerly Tribal Fusion)
- eyeReturn Marketing
- FlashTalking
- Gamut (formerly Cox)
- Google
- I-Behavior
- IDG TechNetwork
- IgnitionOne
- Index Exchange (formerly Casale Media)
- Innovid
- Intent Media
- Krux Digital
- Legolas
- LiveRail
- LiveRamp
- Lotame Solutions
- Madison Logic
- MAGNETIC
- Markit On Demand
- MaxPoint Interactive
- Media Innovation Group (MIG)
- Media.Net
- MediaForge
- MediaMath
- Microsoft Advertising
- Mixpo
- MLN
- Mode Media (formerly Glam Media)
- Netmining
- NetSeer
- Neustar (formerly TARGUSinfo)
- OwnerIQ
- PointRoll
- Prodigity Media
- PubMatic
- Pulsepoint
- Quantcast
- RadiumOne
- RichRelevance
- Rocket Fuel
- The Rubicon Project
- ShareThis
- Sizmek (formerly DG MediaMind)
- Specific Media
- Steelhouse
- TellApart
- The Trade Desk
- Triggit
- TruEffect
- TubeMogul
- Turn
- Undertone
- Vibrant
- Videology
- Vindico
- Xaxis (formerly 24/7 Media)
- Yahoo
- YuMe
- ZEDO
- [x+1]
Training

In 2014, NAI conducted four training sessions about the Code for its members.

NAI kicked off the 2014 annual review with three training seminars in Q1 designed to generally educate members about the Code and the compliance process. During the seminars, NAI staff explained the key requirements of the Code, which went into effect on January 1, 2014, and answered questions about the compliance process in general. In particular, NAI staff reviewed the differences between the 2008 Code of Conduct and the 2013 Code of Conduct in these training seminars. These presentations supplemented the general training NAI staff provided members on individual policy issues throughout the year.

Further, NAI staff provided members with an additional training webinar in early Q2 on best practices for providing and maintaining a consumer choice mechanism - a key component of the NAI's self-regulatory program. The goal of this seminar was to help member companies ensure that they successfully deploy and maintain choice mechanisms, so as to provide the best possible user experience. For instance, NAI staff recommended that members implement real time monitoring systems to check and ensure that members' Opt-Out Mechanisms are functioning properly. NAI staff also identified and highlighted the most common causes of errors with the members' Opt-Out Mechanisms from previous years. NAI staff also provided members with technical guidance around maintaining consistency with the Opt-Out Mechanism, such as how to prepare contingencies for downtime in servers.

In addition to the webinars, NAI staff also provided members with an easy-to-use checklist to help them confirm that they had incorporated the requisite disclosures required by the Code into their privacy disclosures.

Written Questionnaire and Supporting Documentation

Evaluated member companies submitted written responses to an updated 2014 compliance questionnaire. The questionnaire required evaluated member companies to describe their business practices and policies in juxtaposition to the obligations of the Code requirements. Where relevant, the questionnaire also requested that evaluated member companies provide supporting documentation such as sample contract language. The 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;17 other protections for data collected and used for IBA purposes, such as data retention schedules; and processes for oversight and enforcement of contractual requirements.

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

17 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 (§ II.B.3.). This Code requirement is discussed more fully below.
Interviews

Following the review of questionnaire submissions and other supporting materials, at least two NAI staff individuals interviewed representatives from evaluated member companies. Interviews were conducted primarily with high-level management and engineering staff. During these interviews, the compliance team reviewed and probed the evaluated member company’s business and policy issues covered in the questionnaires, including new business lines and the potential use of new technologies to collect data. NAI staff pressed for additional clarification on the calls in the event that questionnaire answers were incomplete, vague, or unclear, or seemingly inconsistent with NAI’s own review of their business model. As appropriate, the NAI compliance team also queried technical representatives about data flows, opt-out functionality, data retention policies and procedures, technologies used for IBA on desktop browsers, and technical measures to prevent the use of PII\(^\text{18}\) by NAI members for IBA purposes.

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 continuously emerge. This holistic view of the industry, resulting from direct engagement with nearly one hundred companies comprising a majority of the ecosystem, enriches 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.

During these interviews, the compliance team took the opportunity to provide evaluated member companies with best practice suggestions. For instance, in a number of cases, NAI recommended that evaluated member companies do more frequent checks of their Opt-Out Mechanism to ensure they function correctly. At other times, the compliance team reminded evaluated member companies of the analysis they may undertake when working with a third party data provider, to help ensure that the data they receive comes from reliable sources. In most cases, NAI provided recommendations on alternative language for privacy disclosures. The compliance team also provided extensive feedback to evaluated member companies to help them improve messaging around opt-out successes or failures due to browser level controls. For example, 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. NAI staff also alerted evaluated member companies of broken hyperlinks in their privacy policies.

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. They also had to attest to the veracity of the information provided in the review process, including any necessary amendments to the questionnaire.

---

\(^{18}\) As defined in the Code, Personally Identifiable Information (PII) includes “any information used or intended to be used to identify a particular individual, including name, address, telephone number, email address, financial account number, and government-issued identifier” (§ I.C.).
The Code requires NAI to publish the results of its annual review, which summarizes members’ compliance with Code and NAI policies (Code § III.B.3). The following sets forth the findings of NAI staff with respect to the 2014 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; 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.
Over the past five years, NAI website had 36,123,843 visits, including 89,223,612 page views. The opt-out page had over 32,897,452 page views.

**EDUCATION**

One main goal of NAI in 2014 was to work with members to expand their efforts to educate consumers about IBA so that consumers can make more informed decisions about data collection and digital advertising. Therefore, it is important for members to explain their complex businesses in simple and clear terms. It is also helpful for members to use common language and definitions in describing their businesses.

Under the education obligation in the Code, members shall use reasonable efforts to take on education efforts individually and collectively. For instance, members collectively educate consumers through the provision of the NAI website, which serves as a centralized portal for offering explanations of IBA and for providing consumers access choice mechanisms. Members also provide links to NAI through their own websites where consumers can learn about the IBA (§ II.A.1.). In 2014, evaluated member companies continued to meet the obligation to both collectively and individually educate consumers about IBA and their available choices.

To collectively educate consumers about IBA, members maintained the centralized and consumer-friendly NAI education site. The NAI education pages provide consumers with a general understanding of the IBA activities of NAI members and the choices available to them. The site also provides a prominent opt out, offers a description of how data may be collected and used for IBA by NAI members, and presents a general description of IBA.

Evaluated member companies also promoted the NAI’s education pages through a digital advertising
In 2014, members donated 5.5 billion impressions to NAI education campaign, tripling the number of donations from members in 2013 and helping lead to over 4.5 million page views on NAI education pages.

campaign, donating over 5.5 billion impressions to the campaign. Collectively, through these various efforts, evaluated member companies expended considerable effort and resources to educate consumers about IBA. The NAI educational campaign helped lead to over 4.5 million page views on NAI education pages in 2014.

Beyond maintaining a centralized consumer education page, the Code further requires member companies to 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. One member, for instance, provides consumers with a “Privacy Manifesto” link on its homepage, explaining its core privacy principles around its data collection and use practices for IBA.

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 Ad Delivery and Reporting practices.

Prominent Notice
First, NAI staff reviewed evaluated member companies’ sites to determine if they met their obligation to provide “prominent” notice. The purpose behind this obligation is to help ensure that consumers can quickly and easily find a link that leads them to information about a member company’s IBA activities and exercise their choice at their discretion.

Overall, NAI staff found that evaluated member companies overwhelmingly provided an easy to find privacy policy in the footer or header of their websites. NAI staff helped ensure that evaluated member companies provide links that were clearly marked as privacy disclosures. For instance, a few evaluated member companies’ privacy disclosures had a link ambiguously labeled “Legal.” NAI staff explained that the link to privacy disclosures could be clearer in conveying the nature and relevance of the information
By working with evaluated member companies, NAI makes it easier for consumers to locate privacy disclosure and choice mechanisms since they are labeled as such.

The vast majority of evaluated member companies also offered a separate and obvious link to an Opt-Out Mechanism. In fact, some evaluated member companies provided a third hyperlink or icon to information about their IBA activities, such as a prominent link to the NAI opt-out page or a “Your AdChoices” link. One evaluated member company even has four links offering consumers information about its IBA activities. The result of the interviews, and the updates to their homepages due to NAI staff feedback, showed that evaluated member companies understood it is key for consumers to be able to quickly and easily locate information on evaluated member companies’ IBA activities.

**Clear and Meaningful Notice**

To meet the “clear and meaningful” requirement, the Code requires that evaluated member companies describe their data collection and use practices in a disclosure 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;
- a data retention statement as well as an Opt-Out Mechanism.

Finally, under the Code, the notice needs to include a statement that the company is a member of NAI and adheres to the Code (§ II.B.1.).

During the annual review, NAI staff assessed the privacy policies and disclosures of evaluated member companies against the descriptions of their business as provided to NAI staff in the compliance questionnaire, and confirmed that these disclosures substantially met Code requirements. Staff also reviewed these disclosures to help confirm that they corresponded with each evaluated member company’s current IBA practices as described by the evaluated member company during their annual compliance review interviews, its corporate site and annual compliance review questionnaire, and news articles.

NAI offered evaluated member companies suggestions to make their privacy disclosures clearer and easier to understand. Further, NAI staff noted that a number of evaluated member companies amended their privacy policies in 2014 in anticipation of the potential, future use of new technologies, such as probabilistic identifiers, for ADR.

---

20 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.

21 As described above, with the creation of the Privacy Disclosures Monitoring Tool, NAI can now monitor member’s privacy disclosures to ensure that members do not inadvertently drop language required by the Code.

22 Evaluated member companies attested to the NAI during the 2014 compliance period that they did not use other technologies for Interest-Based Advertising on desktop browsers.
Pass-On Notice

NAI’s self-regulatory program applies only to its members. Nonetheless, NAI members can help ensure that consumer-facing publisher websites post information about IBA activities occurring on those sites through contractual requirements with those sites’ publishers (§ II.B.3.). These contractual notice provisions are important; they help ensure users are provided with notice at the point of data collection, even when an ad may not be served on that site.23 Based on a review of evaluated member companies’ sample partner contracts, NAI found that evaluated member companies included such contractual requirements when working directly with publishers.24

As part of the evaluated member companies’ overall efforts to promote transparency in the marketplace, members should also make reasonable efforts to enforce contractual notice requirements and to otherwise ensure that all websites where they collect data for IBA purposes furnish notices comparable to those described in section II.B.3 (§ II.B.4.).

NAI found that many members conducted due diligence on websites where they sought to conduct IBA activities prior to working with and/or allowing the website to partner with the evaluated member. Some evaluated member companies trained sales teams to review websites to determine if they had the appropriate notice prior to on-boarding the website as a partner. Other member companies refused to do business with websites unwilling to include the notice while others delayed their sales process until the website implemented the appropriate notice.

Many evaluated member companies also performed random follow-up checks on all or a cross-section of their partner sites. For example, two evaluated member companies reviewed their partner sites on a quarterly basis. Another two evaluated member companies utilized a technical monitoring tool to detect and alert the evaluated member companies if their publishing partners’ notices were inadvertently deleted or altered.25 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 evaluated members terminated relationships on the occasion where the partner’s disclosure was lacking or fell short of Code requirements.

A number of smaller evaluated member companies needed additional assistance around setting up a more robust process in working with website partners. NAI staff determined that the most effective method of helping these evaluated member companies comply with this best practice was to provide them with

23 See the discussion around the “Enhanced Notice Requirement” below.
24 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. 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. NAI found during the compliance review that many such evaluated member companies still took on this best practice step.
25 The Code promotes some best practices for non-NAI companies that help the digital advertising ecosystem as a whole. For instance, an evaluated member company found that a partner site inadvertently dropped its privacy policy from its homepage when the evaluated member company did a check for the partner notice per this provision of the Code. The partner reinserted the privacy policy.
guidelines around procedures to check on partner sites that were feasible with limited resources. These recommendations included regularly checking a reasonably sized sample of the websites where evaluated member companies collected data for IBA to ensure that they provided appropriate notice and following up with those partners that did not.

**Enhanced Notice Requirement**

The Code requires that members provide, and support the provision of, notice in or around advertisements using IBA. That notice provides just-in-time notice by NAI members to consumers, offering yet another means by which consumers can be informed of IBA activities of members and the choices available to them. NAI members continued to lead industry efforts to provide notice and choice to consumers in and around the ads delivered to them by serving an enhanced notice in or around online advertisements trillions of times per month.26 NAI found that those evaluated member companies who lacked the ability to include the standard industry icon or other form of enhanced notice on ads supported the provision of such notice by configuring their systems to support that capability. For instance, some evaluated member companies that are or have platforms do not collect data but facilitate the collection of data by their clients for IBA through their platforms. These evaluated member companies provided their clients with the ability to include this notice on their advertisements through the platform settings.

**Health Transparency**

Members are required to publicly disclose the standard interest segments they use for IBA that are based on health-related information (§ II.B.2.). In this context, standard segments mean those profiles based on health-related information customarily 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 for a specific advertiser or advertising campaign. This Code requirement includes disclosing not just sensitive health segments (such as an inference that a consumer may be interested in a cancer medication), but inferred interests in non-sensitive topics as well, such as diet or fitness. The goal behind a broad disclosure requirement is to allow consumers to make educated decisions about whether to opt out of the collection and use of IBA data by specific member companies. This disclosure requirement is separate and distinct from the Opt-In Consent requirement for sensitive health data discussed in the next section.

Based on responses to the questionnaire and NAI staff review, NAI staff found that, overall, evaluated member companies complied with this requirement in a variety of formats. Some disclosed all standard interest-based segments made available to partners, whether or not the segments were related to health topics, while others listed all health-related segments on pages linked from their privacy policies. NAI agrees

---

26 Because of technical challenges with providing enhanced notice in video advertisements, the NAI is not enforcing this requirement in video advertisements at this time. NAI will make a formal notice before enforcement once the technological challenges are resolved.
that there are a variety of means that this information can be provided in a manner that complies with the Code, and does not require that members use a specific format.

NAI staff found that many evaluated member companies did not offer standard interest segments associated with health topics.\(^{28}\) However, some evaluated member companies did offer custom, non-sensitive health segments for individual advertising campaigns. NAI staff encouraged those members to publicly provide examples of such customized segments as a best practice in order to better educate the public about their activities. Such an evaluated member company would disclose, for example, that it may generate interest segments relating to diet or fitness.

### USER CONTROL - IT’S ABOUT CHOICE

#### 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\(^{29}\) for IBA purposes. Member companies must provide an Opt-Out Mechanism in two discrete locations: on the member’s website and on the NAI website (§ II.C.1.a.). NAI independently confirmed that evaluated member companies provided an Opt-Out Mechanism both on their own website and on the NAI consumer website.

NAI staff did find that a number of evaluated member companies had broken opt out links in their privacy policies or elsewhere on their site, though they did offer functional Opt-Out Mechanisms elsewhere on their site (e.g., the evaluated member companies offered an opt out link to the NAI opt out page). Evaluated member companies worked with NAI staff to quickly fix the broken links.

### HONOR THE 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.). While an opt-out cookie is set and stored on a browser, a member must stop the collection and use of information for IBA on that browser.\(^{30}\) This applies to the collection and use of data for IBA with all tracking technologies, not just cookies.

\(^{28}\) Many evaluated member companies did not employ “standard” interest segments at all, but rather engaged only in practices such as retargeting, search retargeting, and custom segmentation.

\(^{29}\) Non-PII means “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” (§ I.D.).

\(^{30}\) Members may continue to collect data for other purposes, including ADR. For an example, members may continue to collect data from a browser to prevent fraud or to verify that an ad was displayed to that browser.
NAI staff took multiple steps to help evaluated member companies confirm their compliance with this requirement. Evaluated member companies filled out a detailed questionnaire regarding the functionalities of their Opt-Out Mechanisms, including listing the type of technologies they used for IBA. Evaluated member companies were required 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 then manually tested each opt-out cookie to independently evaluate the accuracy of the information submitted on the questionnaire. For example, NAI staff reviewed the behavior of the opt-out scripts, the lifespans of the opt-out cookies, names and values of all opt-out cookies and any potentially unique cookies that were used while an opt out cookie was present on the browser. These tests also looked for opt out functionality issues caused by blocking cookies and certain compatibility requirements on browsers. This review supplements NAI staffs’ regular technical monitoring using the Opt-Out Scanner.31

The questionnaire responses, combined with the manual testing by NAI staff, indicated that evaluated member companies did not continue to collect data for IBA purposes in the presence of an opt-out cookie. In testing, NAI staff noted any cookies with potentially unique identifiers used by evaluated member companies in the presence of an opt out cookie on the browser. If a unique identifier was found, NAI staff asked the relevant evaluated member company about the use of all such cookies. NAI staff confirmed with the evaluated member companies that the cookies were not used for IBA purposes while an opt-out cookie was set.

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 ADR purposes only, such as for analytics, frequency capping, and attribution, as permitted by the Code. NAI staff also tested the opt-outs under various forms of browser cookie blocking features to help ensure that disclosures to consumers were conveyed accurately when an opt out was not functioning as expected.

Evaluated member companies also affirmed in the questionnaire that their Opt-Out Mechanism prevented the collection and use of data for IBA. These Opt-Out Mechanisms applied to data collection for IBA activities for all tracking technologies on desktop browsers.32 More notably, approximately half of evaluated member companies reported that they ceased collecting user-level data in the presence of an opt out. Furthermore, the opt-out cookies set by evaluated member companies had an expiration date at least five-years into the future, as required by NAI.33

31 As detailed above, in 2014, the NAI conducted its technical automated monitoring of member companies opt outs. The testing flagged potential issues with members’ Opt-Out Mechanisms, including the inability for consumers to set opt-out cookies on their browsers. A more thorough discussion of the findings from the automated tool is set forth above.
32 In 2014, the vast majority of NAI members affirmed during the annual compliance review that they exclusively used cookies for IBA on desktop browsers.
33 See http://www.networkadvertising.org/faq/#n178.
Based on the annual questionnaire answers, NAI further found that evaluated member companies had sophisticated systems and policies in place to help verify the effective operation of their opt-out technology. In addition to manual testing of their opt-outs, many evaluated companies had employed automated monitoring tools, conducted regression tests for any software or code changes on their servers, and monitored consumer complaints about opt out functionality through their website. NAI staff reviewed the effectiveness of each evaluated member company’s monitoring program to maintain opt-out functionality, and where necessary, recommended improvements. NAI staff encouraged a number of evaluated member companies to perform additional testing of their Opt-Out Mechanisms.

During the annual compliance review, NAI staff uncovered that an evaluated member company’s opt-out status messaging on its own site was reversed, informing consumers that they were opted-out when the opt-out process had failed, and conversely, reporting that the opt-out process had failed when it had, in fact, succeeded. The issue occurred due to a revision of the company’s site, and was corrected within hours after NAI notified the company. Subsequent reviews of the opt out did not uncover any further problems. The member company’s opt out on the NAI site was not affected by the error at any time. Because the error occurred for a limited time and did not affect a significant amount of consumers, NAI staff and the Compliance Committee, consisting of Board members, did not consider the matter to be a material violation of the Code.

The manual testing, in conjunction with evaluated member companies’ responses to the compliance review questionnaire and their own checks around their opt outs, demonstrated 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 rectified.

**Technologies Used for IBA**

Although the Code is intended to be technology-neutral with respect to the technologies that can be used for IBA, NAI members have historically used HTTP cookies for IBA. Member companies wishing to use any technologies for IBA should do so in compliance with the Code. This includes, at minimum, meeting requisite notice and choice requirements as set forth in the Code.

During the 2014 annual compliance review, NAI staff learned that many evaluated member companies were researching or looking into the use of other technologies for IBA and ADR. Many of these evaluated member companies indicated that they were awaiting further guidance from NAI in order to use other technologies beyond cookies in a manner consistent with the Code. NAI is working with its members to develop policies with

---

See the Introduction and Commentary to the Code.
respect to the use of non-cookie technologies, particularly those that facilitate cross-device tracking, and those that allow tracking on mobile devices.

NAI staff noted during the 2014 annual compliance reviews that a number of evaluated member companies were using other technologies for ADR. NAI also manually evaluated member companies’ activities to look for any locally stored objects set by them. NAI staff worked with evaluated member companies to update their privacy disclosures to reflect the use of these additional technologies for ADR where evaluated member companies notified NAI that they were using additional technologies (§ II.A.2.d.).

NAI staff learned that one evaluated member company briefly used a non-cookie technology for IBA, in limited circumstances. That company’s use of the technology appeared to be consistent with the Code, and its Opt-Out Mechanism appeared to function correctly. Nonetheless, upon learning that NAI was working to develop policies with respect to the use of such non-cookie technologies, the evaluated member company ceased the use of non-cookie technologies for IBA until further guidance from NAI.

**OPT-IN CONSENT**

Under the Code, member companies are required 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 Geolocation Data” and “Sensitive Data” for IBA (§§ II.C.1.d. and e.); and
- material changes to their IBA data collection and use policies and practices (§ II.D.3.).

**Merger**

During the 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 Opt-In Consent under the Code for such merger.35

**Precise Geolocation Data**

The definition of “Precise Geolocation Data” covers the range of technologies, available either now or in the future, which may be able to provide “with reasonable specificity” the actual physical location of a device (§ I.F.) The definition of Precise Geolocation Data excludes more general types of location data, such as postal zip code or city.

NAI staff found during the 2014 annual compliance review that an evaluated member company was using Precise Geolocation Data for IBA on desktop browsers. Accordingly, the evaluated member company attested to NAI staff that it sought to obtain Opt-In Consent for the use of the Precise Geolocation Data

---

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) (§ II.C.1.b.).
for IBA through its publishing partners. (§ II.C.1.d.). NAI will be offering members further guidance on the use of Precise Location for IBA on desktop browsers and the requirement to obtain Opt-In Consent, including what location data is deemed “precise.”

**Sensitive Data**

Once again, NAI staff found that evaluated member companies did not use Sensitive Data for IBA purposes in 2014. Sensitive Data is defined to include specific types of PII that are sensitive in nature, as well as Non-PII related to precise health information and sexual orientation (§ I.G.). NAI also found that evaluated member companies had a uniformly high awareness of using Sensitive Data. Consequently, evaluated member companies had protections in place to ensure that Sensitive Data was not used for IBA.

The Code prohibits serving IBA to consumers (whether through “standard” interest segments, custom segments, or retargeting) based on an inferred interest in sensitive health conditions without a user’s Opt-In Consent. However, 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 outlining how NAI will approach such issues, NAI urged its evaluated member companies to conduct a reasonable analysis of a health condition and determine whether, based on an analysis of all the factors, it should be considered to be a sensitive health segment.

During the annual compliance review, NAI asked a few evaluated member companies to review and change their practices with respect to IBA involving certain health conditions that NAI staff determined may come close to meeting the criteria around a sensitive health segment as 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 health segments of most members in order 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 the 2013 Code of Conduct, NAI added sexual orientation to the list of categories expressly considered “sensitive” under the Code. Thus, the Code now prohibits member companies from using data collected across unaffiliated websites 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.

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.). NAI staff questioned evaluated member companies and reviewed their business models to help identify any potential “material” change relating to their policies and practices around IBA. During the annual review, 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. 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 to use PII for IBA purposes, NAI staff found that not one of the evaluated member companies used PII for IBA purposes.

Evaluated member companies, in fact, set up strong mechanisms to help ensure that they did not collect or receive PII for IBA purposes. First, they often imposed contractual restrictions forbidding their data providers or partners from passing PII to them. They reinforced these contractual requirements through technical controls in the event that PII is passed to them inadvertently. Some evaluated member companies, for example, set up their technical platforms to not accept data with the “@” symbol. This would indicate that the data could include an email address, which is considered PII under the Code. Evaluated member companies generally designed their systems to ensure that any PII that is inadvertently collected is immediately discarded and is not stored or used for IBA purposes.

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 annual review, all evaluated member companies indicated awareness of the sensitivity of data related to children for IBA, and advised NAI that they had processes, policies and procedures in place to ensure that IBA segments specifically targeted at children under 13 are not created or used.37

Every evaluated member affirmed they did not use, or allow the use of, data collected for IBA or ADR for eligibility decisions.

Eligibility

One hundred percent of evaluated member companies affirmed during the annual compliance review that they do not use, or allow the use of, data collected for IBA or ADR for the purpose of determining or making eligibility decisions, such as for health care, insurance, credit, or employment (§ II.D.2.).

TRANSFER RESTRICTIONS

During the annual compliance review, evaluated member companies attested that they were in compliance with the obligation to contractually require any partners to which they provide non-aggregate 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 not attempt to merge such Non-PII with PII held by the receiving party or 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.).

37 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 in 2014 (§ II.F.1.).

Reliable Sources

Evaluated member companies attested, and explained in interviews, that they obtain data from reliable sources (§ II.F.2.). Evaluated member companies reported conducting appropriate due diligence on data sources to help ensure their reliability, including reviews of potential partners’ business practices, particularly of those partners that were not members of NAI. NAI provided several NAI members with basic, general steps and guidance around working with a data source to help confirm its reliability, such as:

- reviewing the data source’s privacy policy;
- understanding the technologies that the data source uses to collect data and whether the data source provides users with appropriate choice, and if applicable, is included on an industry-wide opt out page;
- reviewing the data source’s marketing materials to understand how the data source collects data from users and what types of data it collects.

Reasonable Security

The Code imposes certain requirements designed to help ensure that data collected from IBA activities is adequately secured and is retained only so long as necessary. Evaluated member companies also attested that they were in compliance with the obligation to secure data appropriately (§ II.F.3.).

Retention

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

Independently, NAI staff manually examined the expiration dates of evaluated member companies.

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.
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. In certain cases, NAI staff suggested methods for members to make such disclosures more thorough and accessible. During this process, NAI staff also encouraged evaluated member companies to further reduce their data retention periods, while highlighting the need for data minimization in general.

**ACCOUNTABILITY**

To help ensure compliance with the Code, each member has designated at least one individual with responsibility for managing the member’s compliance with the Code and providing training to relevant staff within the company. (§ III.A.2.) At the outset of the 2014 compliance review process, NAI contacted every member company to help ensure that its contact records are updated as necessary through 2014.

**SANCTIONS**

A detailed compliance assessment process, coupled with strong sanctions, are essential components of the NAI self-regulatory program. Investigations and analysis of alleged violations and review of reports generated through the NAI automated technology tool are completed by NAI staff, which is composed of experienced attorneys and technologists. If NAI staff find during any of the compliance processes that a member company may have materially violated the Code, then they may refer the matter to the Board of Directors with a recommendation for sanctions. If the NAI Board determines that a member has violated the Code, then NAI may impose sanctions, including suspension or revocation of membership. NAI may ultimately refer the matter to the Federal Trade Commission if a member company refuses to comply. NAI may also publicly name a company in this compliance report, and/or elsewhere as needed, when NAI determines that the member engaged in a material violation of the Code.

Although NAI conducted a number of investigations in 2014, NAI staff and the NAI Board of Directors Compliance Committee found that the potential violations did not rise to the level of a material violations of the Code, and that sanctions procedures were not appropriate. Throughout the year, member companies willingly resolved issues raised by NAI staff during the 2014 annual compliance review period, frequently implementing additional measures voluntarily to guard against future noncompliance. 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, helping to ensure the health of the ecosystem.

---

39 For further details about the NAI enforcement procedures, see http://www.networkadvertising.org/pdfs/NAI_Compliance_and_Enforcement%20Procedures.pdf.
SUMMARY OF FINDINGS

In 2014, NAI staff found that evaluated member companies were overwhelmingly in compliance with the Code and that to the extent violations were identified, they were not material. Evaluated member companies showed that they remained highly committed to the NAI’s self-regulatory framework. As in prior years, representatives of the vast majority of evaluated member companies expressed commitment to, and a desire to learn from, the compliance process. They were eager for further guidance from NAI on the use of new technologies and how to best align their business practices with the Code and industry best practices. Many evaluated member companies promptly implemented suggested changes in practices or disclosures suggested by NAI staff during the annual review, even when not strictly required by the Code.
NAI is committed to constantly updating and evolving its self-regulatory program to remain effective. Accordingly, in its 2013 Annual Compliance Report, NAI committed to: (1) work to bring member companies’ practices into alignment with the 2013 Code of Conduct and the Mobile Application Code,\textsuperscript{40} (2) update its education page to more effectively inform consumers about IBA and Cross-App Advertising,\textsuperscript{41} (3) continue to further enhance its technical monitoring, (4) release final guidelines around use of non-cookie technologies and to guide its members and the industry in adapting and moving forward with these new technologies, including for cross-device advertising, with a privacy-centric approach.

\textsuperscript{40} The Mobile Application Code is available at: http://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf.
\textsuperscript{41} As defined in § I.A. of the Mobile Application Code.
MEMBER ALIGNMENT WITH NAI SELF-REGULATORY PRINCIPLES

During 2014, NAI worked with member companies’ to help them bring their practices into compliance with the 2013 Code of Conduct.

NAI provided educational seminars about the 2013 Code of Conduct, giving members guidance on how to continue to remain in compliance with the Code. NAI was also in constant contact with its members, discussing various provisions of the Code. Finally, the annual compliance review helped members ensure that they are in compliance with the Code. NAI will also be releasing a 2015 update to the Code to clarify various aspects of the Code and to further explain how various provisions within the Code may apply in different contexts.

The Mobile Application Code of Conduct was issued in 2013. It covers data collected across mobile applications, rather than desktop websites. The 2013 Code of Conduct will cover data collected on websites accessed by mobile devices when the Mobile Application Code comes into effect. The application and enforcement of the NAI self-regulatory principles across mobile devices (including mobile web browsers and mobile applications) is scheduled to begin sometime in 2015, since technical measures to evaluate compliance with the recommended practices are not yet fully integrated into the NAI compliance program. Therefore, this compliance report does not address compliance with the Mobile Application Code, which has not yet gone into effect.42 NAI will provide advance notice to members of the expected implementation date of the Mobile Application Code. Consumers will

2014 NAI Initiatives:

• 2014 draft NAI Guidance for the Use of Non-Cookie Technologies was released to members for their review.

• Privacy Disclosure Scanner was implemented and used.

• Next-generation technical compliance tool under development.

---

42 The NAI is currently working with members to bring them into compliance with the Mobile Application Code and is accepting membership applications from mobile networks, exchanges, and other ad tech companies specializing in mobile advertising. It is also working with existing members to bring their mobile advertising services into compliance with the Mobile Application Code. New members will go through the standard pre-certification process to help confirm that they are in compliance with the Mobile Application Code prior to joining the NAI. Existing members engaged in IBA on mobile devices worked with NAI staff throughout 2014 to help them prepare to bring their operations into compliance with the Mobile Application Code prior to it going into effect sometime in 2015.
benefit from enhanced transparency and control in the mobile world as they increasingly use tablets, smart phones, and other mobile devices to engage with brands, content, and digital services.

In preparation for the coming implementation of the Mobile Application Code, during the 2014 compliance assessments, NAI worked with a number of members to review their activities on mobile devices. NAI will provide members with further education seminars to review the Mobile Application Code.

UPDATE TO EDUCATION PAGES

In July 2014, NAI launched an initiative to update its consumer education pages to reflect that its members’ business models and technologies have evolved and there are countless new innovative consumer products and services in the marketplace. NAI created a working group of company representatives to update the content and messaging on the NAI website. The new consumer education pages are set to be finalized in Q2 of 2015.

TECHNICAL MONITORING

NAI reworked and enhanced its technical tools in 2014 to detect opt-out issues and streamlined NAI staff’s reviews of reports generated using the technical tools. NAI also added a Privacy Disclosure Scanner that regularly reviews privacy policy pages for any changes made to the disclosure that may lead to a potential compliance issue.

With NAI’s plan to cover mobile devices and non-cookie technologies under its enforcement in the future, NAI is upgrading its compliance software to be compatible with this transition. NAI began using a beta version of the next-generation compliance software on February 2015. NAI added the following functionalities and features to the tool:

- A large suite of research and forensics tools, including the detection of anomalies on members’ web activities and opt-outs, which helps NAI staff navigate diverse methods of data collection to help identify new methods of data collection by members.

- Support for in-depth analysis of 30 types of data collection methodologies other than cookies, including pixel tags, headers, images, EXIF data, JavaScript key-value pairs, URL queries, phone contacts, text message data, and more. This helps NAI staff broadly understand the various data collection methods by members, including the behavior of non-cookie technologies, such as HTML5 local storage, statistical identifiers, and mobile identifiers.

- Support for monitoring and analyzing web traffic on a wide range of platforms, such as mobile phones, mobile browsers, tablets, web browsers, and desktop applications. The compliance software is compatible with most devices that can connect to the Internet.

- A number of smaller improvements, such as the expansion of web crawls from 200 pages to nearly
1 million web pages while simulating the likelihood of a human visiting any of those websites. In addition, unifying multiple tools under the same Graphic User Interface and next-generation database helps enable NAI to quickly add new analyses in response to new business models and compliance issues.

This upgrade allows NAI staff to continue enforcement of the Code as members explore new technologies and platforms. With the upgraded compliance software, NAI will 1) continue its testing for opt-out issues while detecting new types of compliance issues (such as collection of Personal Directory Data), 43 2) review detailed reports of members’ privacy disclosure revisions and changes in data collection practices on desktop and mobile devices, and 3) investigate compliance issues on mobile devices and with members’ use of non-cookie technologies.

**GUIDELINES FOR NEW TECHNOLOGIES**

Because the Code is “technology neutral,” members may use any technology for IBA or ADR as long as they meet the requirements of the Code. 44

In 2013, to address various changes and challenges in the industry, NAI convened a working group to develop guidelines to address the potential use of other technologies for IBA. NAI tackled the challenging policy issues surrounding the use of non-cookie technologies with its members. The group released draft “NAI Guidance for the Use of Non-Cookie Technologies” for membership review in late 2014. The draft guidance outlines how members may use these non-cookie technologies in a manner consistent with the Code. NAI continues to evaluate member feedback on the guidance document. It is NAI’s goal in 2015 to help those members that choose to adopt these technologies to use them in conformance with the Code once the final guidance is adopted and goes into effect.

---

43 As defined in § I.I of the Mobile Application Code.
44 The Code does not currently cover IBA activities on mobile devices or mobile companies. As a result, NAI staff’s review and testing was limited to desktop devices.
Through this report, NAI provides transparency into its various compliance efforts in reviewing member practices and helping to confirm that members observe the obligations of the Code. This report proves, once again, that NAI has enhanced the overall health of the digital advertising industry through this rigorous process - including on-boarding, educational seminars, various technical monitoring tools, questionnaire reviews and member interviews. This comprehensive process is designed to help NAI and members detect potential Code violations as soon as possible, and to protect consumers by helping make sure member companies adhere to the Code. NAI staff also consults directly with members throughout the year, providing guidance as needed. NAI technical tools help enable the NAI staff to regularly monitor member activities in order to help them continue to comply with the Code.
While NAI is pleased with its efforts to improve its self-regulatory program and the hard work of its members to comply with the Code, NAI constantly seeks to improve its program.

During 2015, NAI plans to finalize its education page to more effectively inform consumers about IBA and Cross-App Advertising in the mobile world. NAI will also release updated versions of the 2013 Code of Conduct and the Mobile Application Code, which are intended to clarify certain obligations present in the Code, in response to questions received by NAI staff from members.

As the industry moves quickly toward the use of new technologies in the digital advertising space, NAI’s goal in 2015 is to release final guidelines around use of these technologies and to guide its members and the industry in adapting and moving forward with these new technologies, including for cross-device advertising, with a privacy-centric approach.

This includes the development of a new opt out page for members and consumers to facilitate consumer choice as IBA technologies move beyond HTTP cookies and a new member portal to help NAI manage member on-boarding, training and communication.

Further, NAI staff did not review member activities to link devices during the 2014 annual compliance review as these activities are not covered by Code. For instance, the Code does not cover the activity of linking devices based on the assumption that the devices belong to the same user or household. NAI will begin working to develop policies in line with the related business practices that are emerging with the maturation of technologies that facilitate the linking of devices presumed to belong to the same user or household. The NAI will work with members to develop and issue guidance in the future regarding the application of the Code, including the application of the Opt-Out Mechanism to the collection of data across

NAI will be working throughout 2015 to update its monitoring tools and processes in an ongoing effort to make its program even stronger.
devices and/or the linking of multiple devices used or likely used by the same individual or household. NAI has worked with several members to help them deploy these business models with the current privacy principles set forth in the Code in mind, including notice, choice and accountability.

All these new developments in technologies and data collection methods have resulted in additional new interest in NAI membership as companies look to collect and use data in a responsible manner. In fact, NAI admitted 3 members in January 2015 alone.

NAI staff acknowledges that there are challenges ahead in 2015. The industry is becoming more sophisticated, complicated and intertwined. New business models are being created at a rapid pace. Members are able to collect data from new sources using new methods. With the help of its Board and its members, NAI will move forward to work with members to further develop best practices for the collection and use of data for IBA across the ever-evolving digital world.