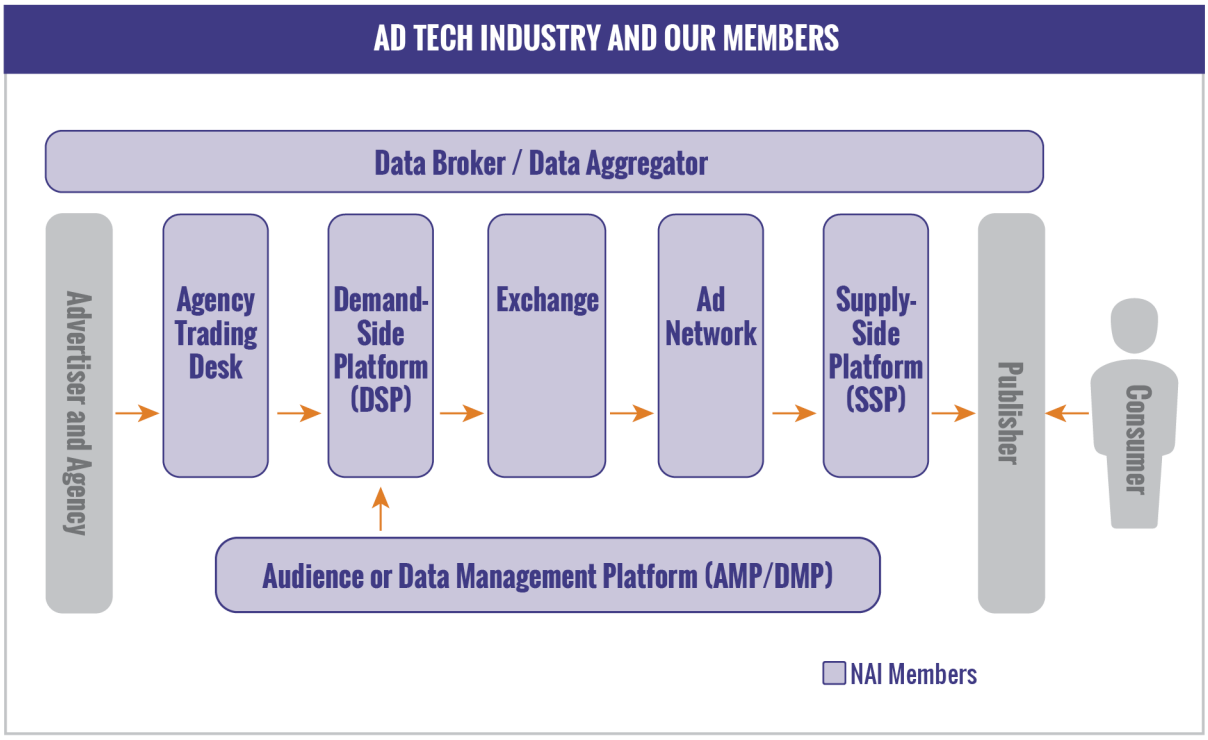
2016 ANNUAL COMPLIANCE REPORT

NAI
Network Advertising Initiative

TABLE OF CONTENTS

INTRODUCTION

Since 2000, the Network Advertising Initiative (NAI) has been a leading self-regulatory body governing "third parties" engaged in Interest-Based Advertising (IBA)[1] and Ad Delivery and Reporting (ADR)[2] in the United States, based on its Code of Conduct (Code).[3] In 2016 the NAI also began regulating Cross-App Advertising (CAA)[4] by enforcing its Mobile Application Code (App Code). At the time of publication, the NAI has 108 member companies. NAI members include a wide range of businesses such as ad networks, exchanges, platforms,[5] data aggregators, and other technology providers. Across websites and mobile applications, these intermediaries form the backbone of the digital advertising ecosystem—helping advertisers reach audiences most likely to be interested in their products and services while allowing consumers to receive ads that are relevant to their interests. This relevant advertising, in turn, continues to power free content and services in the digital ecosystem, including websites and mobile applications.[6]



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

This report provides a summary of the NAI's achievements in 2016 as well as staff's findings from the 2016 compliance review. During the 2016 compliance period, NAI staff reviewed members' compliance with the Code[7] and the App Code[8] (together, Codes). This report is intended to provide consumers, regulators and others with visibility into the NAI's compliance program and self-regulatory process. In addition, this report helps illustrate how the compliance process shapes the evolution and goals of the NAI's policies and procedures, to ensure that the NAI continues to offer a vibrant self-regulatory program that responds to new issues and technologies in a practical way.

2016: A YEAR IN REVIEW

The NAI's self-regulatory program continues to evolve, mature, and expand. The NAI set forth its goals for the following year in its 2015 Annual Compliance Report. As part of that process, the NAI committed to: (1) further enhance its education materials to more effectively inform consumers about new technologies and data collection across mobile applications; (2) work on synthesizing the Code and App Code into one document; (3) explore the potential for guidance regarding cross-device linking for digital advertising purposes; (4) launch a revised NAI opt-out tool, enabling consumers to view status and exercise choice even in the presence of non-cookie technologies used for IBA; and (5) enhance the role of technical monitoring in the mobile and non-cookie spaces.

In 2016, 27 companies applied for membership in the NAI, and 19 new members were approved by the Board of Directors.

The NAI expanded its consumer education materials throughout the year, with a focus on non-cookie technologies and mobile advertising. In May 2016 the NAI launched detailed instructions on the use of privacy-related platform controls available on the vast majority of mobile devices.

NAI staff and its Board of Directors worked to combine the Code and App Code into a single document, continuing those efforts into 2017 with substantive changes that better reflect the newest business lines and products from NAI members. The NAI aims to publish these updated Codes as one document once it is finalized. Similarly, the NAI staff and Board continued work on cross-device linking policy throughout 2016, leading to the 2017 publication of the *Guidance for NAI Members: Cross-Device Linking* (Guidance on Cross-Device Linking). This document updates NAI policy by requiring members to apply the principles present in the NAI Codes, including notice and choice, to cross-device linking for digital advertising purposes.

In 2016 the NAI also continued to develop its revamped opt-out tool, focusing on enhanced functionality and transparency in situations involving third-party cookie blocking and the uses of non-cookie technologies. NAI staff onboarded member companies onto the tool and also worked with the Digital Advertising Alliance (DAA) to make the tool available to users of the DAA's AboutAds.info site. The new opt-out tool launched on the NAI and DAA sites in early 2017.

Also in 2016, the NAI hosted its fourth annual Summit, bringing this one-of-a-kind industry event to the West Coast for the first time, in San Francisco. This annual event provides member companies with an opportunity to join robust discussion about the latest technologies, regulatory and legislative trends, and emerging business models. The 2016 Summit featured Federal Trade Commission (FTC) Director of the Bureau of Consumer Protection, Jessica Rich, as well as Special Assistant Attorney General of California, Justin Erlich.

The 2016 Summit featured Federal Trade Commission (FTC) Director of the Bureau of Consumer Protection, Jessica Rich, as well as Special Assistant Attorney General of California, Justin Erlich.

The NAI continued the development of its technical monitoring tools, in an ongoing effort to increase efficiency and keep up with evolving technologies. Some of these efforts were focused on automating processes on mobile devices and monitoring the various types of data points accessed or requested by NAI members in mobile applications. The resulting insights enabled NAI staff to probe deeper into members' mobile data collection practices and to request more detailed responses to the compliance questionnaire in 2016.

NAI members and staff, together with the NAI Board of Directors, worked throughout the year to identify the most pressing privacy issues associated with data collection and use for targeted advertising on television sets. During this time, the NAI worked closely with FTC. The NAI hosted a roundtable event for its members and FTC staff to discuss policy and technology issues in the connected TV space. NAI staff also participated in the November 2016 FTC Smart TV Workshop.[9]

Twenty-seven companies applied for NAI membership in 2016, and nineteen companies were approved as new members by the NAI Board of Directors. This strong membership growth demonstrates that effective self-regulation continues to be a vital component in building trust not only between the advertising technology industry and consumers, but also between member companies and service providers, publishers, and advertisers.

THE NAI COMPLIANCE PROGRAM

JOINING THE NAI: COMPLIANCE BEGINS EVEN BEFORE MEMBERSHIP

Companies interested in NAI membership cannot simply join the NAI; they must commit to compliance. At least two members of NAI staff, with legal and technological expertise, evaluate each applicant's business model and privacy practices. These reviews focus on the applicant's responses to the application questionnaire, its privacy disclosures, and information regarding its data collection, use, retention, and sharing practices, to ensure these are consistent with the Codes. Additionally, a NAI technologist evaluates the applicant's consumer choice mechanisms and data collection practices. NAI staff then conducts interviews with high-level employees at the company, asking further detailed questions, including those aimed at resolving potential discrepancies identified from the application materials, or assessment of business practices that may be inconsistent with the Codes.

Companies can't simply join the NAI; they must commit to compliance.

An applicant that wishes to complete the application process must work with NAI staff to bring its relevant services and products into a position to comply with the Codes. NAI staff evaluates each applicant's practices and disclosures, highlighting those that need to be addressed before the company can become a member of the NAI. Though some companies attain membership within a few weeks, this assessment can often be a months-long process, with the NAI providing guidance and suggestions about compliance along the way. Many applicants make substantial revisions to their public privacy disclosures to provide the full level of notice required by the Codes as a result of the NAI application review process. Typically, NAI staff provides technical guidance to help an applicant develop an Opt-Out Mechanism[10] that is both capable of meeting the Codes' requirements and be compatible with the NAI opt-out page. At times, applicants have abandoned or dramatically revised entire lines of business that did not, or could not, meet the requirements of the Codes.[11]

Once this pre-membership review is completed, NAI staff submits a recommendation for membership to the Membership Subcommittee of the NAI Board of Directors, followed by the full Board. The NAI Board of Directors is comprised of seasoned attorneys and compliance executives from fourteen leading member companies. The Membership Subcommittee of the Board reviews each application, often requesting additional information from an applicant, before recommending acceptance of a new member to the full Board. Therefore, each potential member is reviewed first by NAI staff, second by the Membership Subcommittee, and finally by the full NAI Board. This review process helps establish that an applicant has administrative, operational and technical capabilities that can comply with the requirements of the Codes *before* the company may claim membership in the NAI.

In 2016, nineteen companies[12] completed the application process and were approved for membership by the Board.

At the close of the 2016 compliance review period, the NAI Board consisted of:

Douglas Miller, NAI Chairman; Vice President and Global Privacy Leader, AOL Advertising

Alan Chapell, NAI Vice-Chairman; President of Chapell and Associates, representing Audience Science

Matthew Haies, NAI Secretary; Senior Vice President & General Counsel, Xaxis

Shane Wiley, NAI Treasurer; Vice President of Privacy & Data Governance, Yahoo!

Brooks Dobbs, Chief Privacy Officer, KBMGroup

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

Ted Lazarus, Director, Legal, Google

Ari Levenfeld, Chief Privacy Officer, Rocket Fuel, Inc.

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

Andrew Pancer, Chief Operating Officer, Dstillery

Mark Partin, Managing Counsel, Privacy and Security Legal, Oracle

Noga Rosenthal, Chief Privacy Officer, Conversant/Epsilon

Julia Shullman, Senior Director, Deputy General Counsel, Commercial & Privacy, AppNexus

Estelle Werth, Global Privacy Officer, Criteo

MONITORING OF MEMBERS

NAI Technical Monitoring

Once companies demonstrate their ability to comply with the Codes, and become members of the NAI, they must remain in compliance[13] so long as they maintain their membership. One way the NAI helps facilitate this process, even in between annual compliance reviews, is through its automated monitoring suite including an Opt-Out Scanner and Privacy Disclosures Scanner that allow staff to flag potential issues for review or investigation.

One of the main benefits of these automated monitoring tools is the ability to help NAI staff spot and remedy potential problems quickly, thus enabling the NAI to address concerns with members before they become widespread and affect large numbers of consumers. The issues flagged by the monitoring tools included revisions to privacy policies and new opt-out behavior. Upon further review, NAI staff typically confirmed that these flags did not point to violations of the Codes. A common example is that of a flag that may have been raised when a privacy policy appeared to be inaccessible, though further investigation demonstrated that the disclosures in question had been moved to a different URL and continued to be accessible to consumers.

As in prior years, on a number of occasions the NAI's monitoring tools flagged actionable issues that could have resulted in violations of the Codes if left unaddressed. For example, one evaluated member company removed its data retention policy from its disclosures during a website redesign. Such issues were generally resolved by member companies shortly after notification by NAI staff. None of these instances were considered to rise to the level of non-compliance with the Codes because the underlying issues were resolved quickly, were found to be unintentional, and affected a limited number of consumers. NAI staff noticed at least one evaluated member company inadvertently removed several key disclosures, although these were promptly replaced once NAI staff notified the company's representative. Additionally, where applicable, NAI staff suggested methods through which members could not only address existing issues but also prevent them from recurring in the future. In 2016 many evaluated member companies updated privacy disclosures to account for their participation in the US-EU Privacy Shield framework, which in turn prompted several members to reach out to NAI staff for guidance on other related disclosure updates.

Web-based Opt-Out Testing

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

The NAI also scans member opt outs through proprietary software.[14] This NAI proprietary Opt-Out Scanner collects information about the cookies set via the NAI opt-out page and generates a short report, helping staff to recognize when required opt-out cookies are not set, are overwritten, or otherwise deleted. Such problems are exceedingly rare, though they can be the result of incomplete server migrations and potential bugs in new products and services.

Additionally, the NAI receives consumer emails regarding specific functionality issues that are difficult to identify with in-house testing, such as temporary malfunctions on load-balancing servers that affect only certain regions.

This holistic approach helps the NAI to identify and address most potential problems with member Opt-Out Mechanisms. The combination of monitoring, daily manual testing, and review of consumer emails helps the NAI and its members limit opt-out downtime and to resolve opt-out issues before they result in non-compliance with the Codes.

Privacy Disclosures Scanner

In 2016 the NAI Privacy Disclosures Scanner monitored over 200 pages for changes that could affect member compliance with NAI disclosure requirements.

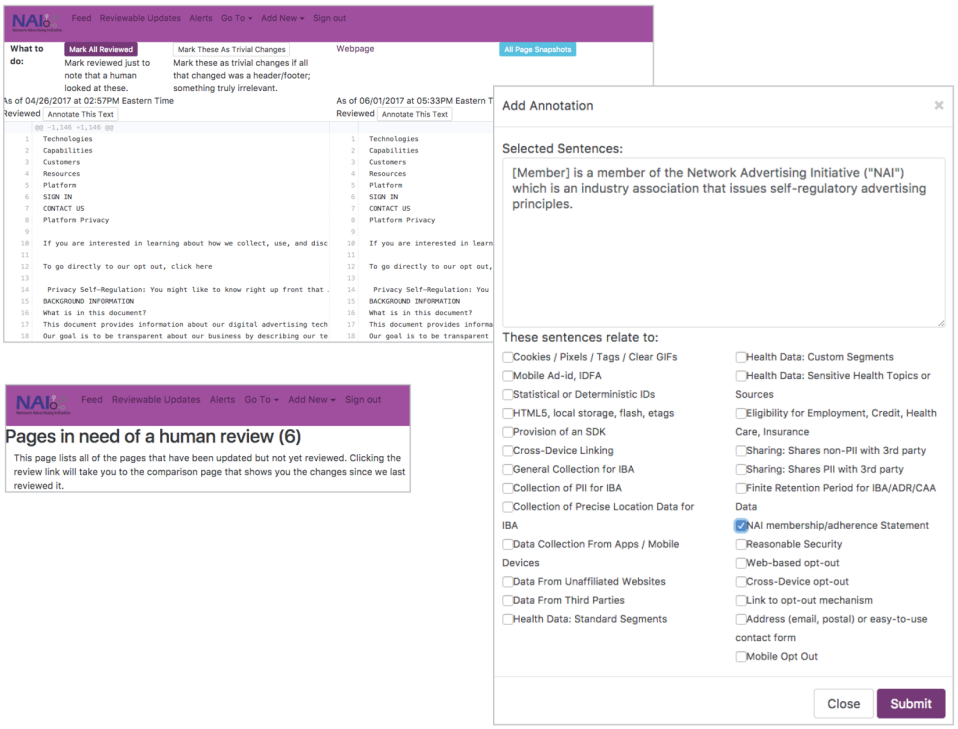
The NAI Privacy Disclosures Scanner scans member companies' web pages for privacy policy and other disclosure modifications, as well as errors in accessing those pages. These scans help NAI staff identify a variety of potential compliance issues, including incomplete or missing disclosures, broken links, or non-conforming Opt-Out Mechanisms. NAI staff works with members to promptly address such inconsistencies.

The Privacy Disclosures Scanner helped bring numerous business model changes to the attention of NAI staff, such as new products offered by NAI member companies, and acquisitions of new brands and business lines. Because disclosures in privacy policies usually occur in anticipation of the launch of a new product, spotting these changes allowed NAI staff to help members evaluate how the Codes apply to these new products and offerings. This knowledge, in turn helps the NAI further optimize its monitoring tools and aids NAI staff in incorporating new concepts into the following year's annual compliance reviews.

Many of the changes to members' privacy disclosures continued to be positive. In other words, many of the changes were the result of members responding to action items and feedback provided by the NAI staff, or members proactively disclosing a new product or technology.

To the extent member revisions to their privacy policies implicated disclosures that are required by the Codes, these were addressed and made to comply with the NAI requirements within a reasonable time from NAI staff's notice to the member. NAI staff continues to acknowledge that members face the difficult task of explaining to consumers in a clear yet meaningful manner what data they are collecting and using for advertising purposes. The NAI also recognizes that members must balance the need to be concise with the need to provide thorough disclosures. NAI staff applies its extensive knowledge of the industry, understanding of the Codes, and expert judgment in determining the relative adequacy of the disclosures in a member's privacy policy from an NAI Code perspective.

MONITORING TOOL PERFORMING A SAMPLE ANALYSIS OF A PRIVACY POLICY



In 2016 the NAI received over 6000 consumer queries through its website or via email.

Investigating Consumer Communications

NAI Website

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

In 2016, the NAI received and reviewed approximately 6050 queries through its website, and approximately 260 contacts via telephone. This is a small increase from the amount of queries received in 2015. NAI staff determined that, as in the past, the majority of the inquiries received did not pertain to issues within the scope of the NAI's mission. For example, many emails were comprised of questions about junk email, attempts to reach the publishers of specific websites, or other issues not covered by the Codes.

Fewer than 30 percent of consumer inquiries were related to the NAI, the NAI Codes, or NAI member companies. The vast majority of these inquiries were requests for assistance in troubleshooting technical issues with IBA opt outs, particularly in cases where browser controls blocked third-party cookies, or ISP/workplace Internet filters or anti-virus software prevented opt-out cookies from being set on the consumer's browser. In several instances, consumers notified the NAI of specific opt-out issues, and helped confirm potential problems with recognizing opt-out requests flagged by the NAI's monitoring tools.

In 2016, consumer inquiries led to one NAI compliance investigation regarding a member company's opt-out functionality. The NAI technical team was unable to duplicate the consumer's opt-out problem, which appeared to have been resolved by the company.

In summary, NAI staff determined that consumer communications received by the NAI in 2016, through email, phone, or the website that were conducive to resolution by the NAI as part of its compliance reviews had been resolved within a reasonable timeframe. There were no allegations of member noncompliance with the Codes that NAI staff determined to be material in nature.

Consumer Question Mechanisms

NAI staff tested members' compliance with section III.C.2 of the Code and App Code, which requires members to offer a mechanism for consumers to submit questions or concerns about the company's collection and use of data for IBA and CAA. NAI staff found that all evaluated member companies provided an email address, web-based form, or troubleshooting guide tied to a forum for consumers to use if they wished to inquire about the company's privacy practices.

NAI staff also independently tested member responses to consumer questions sent through these question mechanisms. NAI staff sent three rounds of test emails to member companies with standardized questions about opting out of IBA or CAA. Of the evaluated member companies, after three rounds of testing 98 percent replied promptly and with informative responses about their IBA or CAA activities.

In those instances where NAI staff did not receive a response, or received a response that was inadequate, the evaluated member companies were notified of the problem and were typically able to resolve the underlying issue in a swift manner. Lack of responsiveness was often caused by junk email filtering. Importantly, all evaluated companies also provided a link to the NAI's opt-out page, thus ensuring that consumers could pose questions and send complaints through the NAI's own consumer question mechanism. The NAI thus provides a back-up means for consumers to voice privacy questions and concerns regarding member companies' data collection and use for IBA and CAA.

Investigating Other Complaints

In addition to the NAI's own monitoring and research, NAI staff also scrutinizes a variety of other sources for potential instances of member non-compliance, including published articles, public allegations by privacy advocates, complaints to NAI by third parties or other NAI members, and investigations by other regulatory bodies. In 2016, NAI staff conducted one investigation based on public allegations of potential non-compliance with the Codes. The allegations, made in 2016, indicated that an NAI member company did not provide adequate notice in or around targeted advertisements, did not provide notice of its IBA activities in its own privacy disclosures, and did not provide a functional link to an Opt-Out Mechanism.

This investigation, like other reviews during this compliance period, included an examination of the alleged practices under the Codes, discussions with the relevant member company, and a review of public and non-public facts. NAI staff determined that the alleged violations published in 2016 involved practices that occurred several years prior to their publication, and that any alleged non-compliance had already been cured by the time the company joined the NAI as a member in 2014. NAI staff did not observe the problems subsequently resurfacing after the company joined the NAI. Consequently, the allegations did not constitute a violation of the Codes.

ANNUAL REVIEW

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

During the 2016 annual compliance review, NAI staff reviewed the 89 companies that were members from January 1 through December 31, 2016.[15] These members are referred to as "evaluated member companies" throughout this report. Those members that joined the NAI after January 1, 2016[16] were already subject to an extensive review during the calendar year as part of the on-boarding process, and therefore were not part of the 2016 annual compliance review. Those members will be assessed again during the 2017 annual review process.[17]

Training

In 2016, the NAI provided a number of training and educational sessions for its members, including webinars and staff visits to member company offices.

The NAI started 2016 with a training webinar designed to educate members about the 2015 Update to the NAI Mobile Application Code. During this webinar, NAI staff explained the key requirements of the updated App Code, enforced beginning January 1, 2016. In particular, NAI staff reviewed the differences between the Code and the App Code, and focused on mobile-specific issues such as advertising identifiers, platform controls, and Precise Location Data. This presentation was intended to supplement the general training NAI staff provided members on individual policy issues throughout the year.

In total, the NAI averaged one all-member call per month in 2016, including educational calls featuring outside law firms and other self-regulatory bodies. NAI staff also made a number of visits to member company offices, and the offices of law firms advising members across the United States in order to provide in-person training and education regarding the Codes' requirements and ongoing developments.

Written Questionnaire and Supporting Documentation

Evaluated member companies submitted written responses to a thoroughly revised 2016 compliance questionnaire. The questionnaire required evaluated member companies to describe their business practices and policies in relation to the requirements of the Codes. In 2016 this questionnaire included, for the first time, the requirements and best practices in the App Code. Where relevant, the questionnaire also requested that evaluated member companies provide supporting documentation such as sample contract language, links to specific disclosures, and lists of cookies or other identifiers. Building on information obtained from prior reviews, this questionnaire also covered such issues as the collection and use of data for CAA purposes, in addition to IBA; policies governing those practices; contractual requirements imposed on business partners concerning notice and choice around IBA and CAA activities;[18] other protections for data collected and used for IBA and CAA purposes, such as data retention schedules; and processes for oversight and enforcement of contractual requirements. At the end of the compliance review period, the NAI required members to sign attestation forms to confirm their responses continued to be accurate to the best of the member's knowledge.

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

Interviews

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

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

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

Attestations

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

EVALUATED MEMBER COMPANIES

33Across
Accuen
AcuityAds
Adara
AddThis
Adobe
AdRoll
Aggregate Knowledge
AOL Advertising
AppNexus
Atlas
Audience Science
BAM
BazaarVoice
BlueCava
BlueKai
BrightRoll (Yahoo)
ChoiceStream
Circulate
Collective
Conversant
Criteo
Cross Pixel Media
Datalogix
DataXu
Datonics
Defy (Break) Media
Drawbridge
DStillery
Exelate
Exponential/Tribal Fusion
eyeReturn
EyeView
Flashtalking
Gamut
Google
GumGum
KBM Group
Ignition One and Netmining
Index Exchange
Innovid
Intent Media
Kargo
Krux
LinkedIn
Lotame
Madison Logic
Magnetic
Markit on Demand
MaxPoint
Media.net
MediaForge
MediaMath
Microsoft
MIG
Netseer
Neustar
Optimatic
OwnerIQ
Parrable
Pubmatic
PulsePoint
Quantcast
RadiumOne
RhythmOne
Rocketfuel
Rubicon
RUN
ShareThis
Simpli.fi
Sizmek
Steelhouse
Tagular
TapAd
Tellapart
Trade Desk
TruEffect
TubeMogul
Turn
Undertone
Varick Media Management
Viant
Vibrant
Videology
x+1
Xaxis
Yahoo
Yieldmo
YuMe

2016 ANNUAL REVIEW FINDINGS

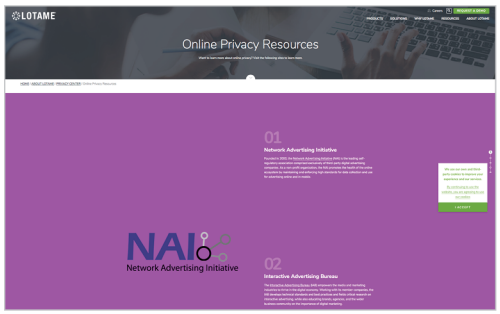
The Codes require the NAI to publish the results of its annual review, providing an opportunity for the NAI to summarize members' compliance with the Codes and NAI policies (Code § III.B.3.; App Code § III.B.3.). The following section presents the findings of NAI staff with respect to the 2016 annual review. This section also more fully summarizes the obligations imposed by the Codes, but does not restate all principles set forth in the Codes, and as such it should not be relied upon for that purpose. The full Codes, including definitions of relevant terms, can be found through the links provided in this report.

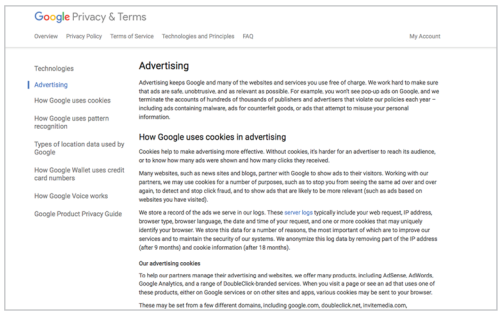
Evaluated member companies estimate that they have collectively provided billions of impressions to the NAI's educational campaign.

EDUCATION

The Codes stipulate that members should use reasonable efforts to educate consumers about IBA and CAA, and require members to maintain an NAI website to educate consumers (Code § II.A.; App Code § II.A.). It is key that the NAI provides a centralized education page that members may point to, implementing uniform terminology to help explain what can be a complex ad tech ecosystem to consumers. Accordingly, all members collectively educate consumers through the provision of the NAI website, which serves as a centralized portal for explanations of IBA, CAA, and associated practices, as well as for providing consumer access to choice mechanisms. Members provide links to the NAI through their own websites, where consumers may also learn about IBA and CAA. In 2016, evaluated member companies met this obligation to collectively educate consumers about IBA, CAA, and available choices with respect to data collection for these purposes.

SAMPLES OF MEMBERS' OWN EDUCATIONAL MATERIALS





Evaluated member companies also continued to promote the NAI's education materials through a digital advertising campaign, estimating that they've collectively donated billions of impressions to the campaign.

The NAI has developed a new and revamped consumer education campaign, reflecting a shift in the industry toward mobile ecosystems, non-cookie technologies, and the linking of devices for advertising purposes. The NAI is launching this updated campaign in 2017 in order to educate consumers about the privacy implications of the latest developments in these technologies, and the most recent updates to NAI guidance. Accordingly, the NAI anticipates increased impression donations from members and a corresponding increase in consumer use of its educational materials going forward.

Beyond maintaining a centralized consumer education page, the Codes further suggest that member companies should individually educate consumers about IBA, CAA, and the choices available regarding data collection for these purposes (Code § II.A.2.; App Code § II.A.2.). NAI staff found that evaluated member companies provided information regarding the technologies used for IBA and CAA, as well as a clear link to a consumer choice page. In addition, NAI staff found that multiple 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 and CAA activities and provided consumers with an easy to locate choice mechanism.

Several NAI members also play key roles in the Federation for Internet Alerts (FIA)[20], which uses digital advertising technology for the common good, distributing life-saving information to the right viewers at the right time, including missing child Amber Alerts and severe weather warnings. During the 2016 election, NAI members participated in the PEW Voting Information Project,[21] helping to ensure that voters could access information regarding their polling locations and local ballot initiatives. Leveraging digital advertising technology for public service is an extension of the broader education efforts undertaken by NAI members.

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

TRANSPARENCY AND NOTICE

Member Provided Notice

The Codes require members to provide "clear, meaningful, and prominent notice" on the member's website describing their IBA, CAA, and/or ADR practices (Code § II.B.1.; App Code § II.B.1.).

Clear and Meaningful Notice

The Codes require that evaluated member companies publicly disclose their IBA, CAA, and ADR data collection and use practices in an understandable manner. This includes, as applicable, providing a description of the IBA, CAA, 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, CAA, and/or ADR activities;[22] a data retention statement; and an Opt-Out Mechanism. Finally, the Codes require members to disclose that the company is a member of the NAI and adheres to the Codes (Code § II.B.1.f.; App Code § II.B.1.f.).

During the 2016 annual review, NAI staff assessed the privacy policies and other privacy-related disclosures of evaluated member companies in juxtaposition with current IBA, CAA, and ADR practices as described in each company's annual interview, its corporate site, annual compliance review questionnaire, business model changes discovered through ongoing technical monitoring, and news articles.[23] Where appropriate, the NAI offered evaluated member companies suggestions to make privacy disclosures clearer and easier to understand. Further, NAI staff noted that evaluated member companies amended their privacy policies in 2016 to reflect the use of newer technologies for IBA and ADR, and to provide more information about data collection and use for CAA and ADR on mobile devices.

As this was the first annual compliance review to include mobile-specific disclosures as required by the App Code, numerous NAI members did not initially provide all of these disclosures, or provided them in a manner that may not have been clear to consumers. The NAI took additional steps to educate members regarding required and suggested disclosures pertaining to advertising identifiers on mobile devices, the choice mechanisms available on mobile platforms, and location data. NAI staff noted considerable improvement in mobile-specific disclosures throughout the year and will again work with members in 2017 to apply privacy policy insights gained during the 2016 review.

Prominent Notice

In 2016 NAI staff reviewed the websites of evaluated member companies to determine if they met the obligation to provide "prominent" notice. The purpose behind this obligation is to help ensure that consumers can quickly and easily find a link leading to information about a member company's IBA activities, and to exercise choice regarding IBA at their discretion.

As a result of ongoing educational efforts during prior compliance reviews, NAI staff found that at the time of their 2016 reviews, all evaluated member companies provided an easy to find link to privacy disclosures in the footer or header of their websites. Throughout the year, NAI monitoring tools alerted staff to several instances of potentially malfunctioning privacy links due to changes such as altered URLs, clerical errors, or website redesigns.

Nearly all evaluated member companies offered a separate and obvious link to an Opt-Out Mechanism, a prominent link to the NAI opt-out page, or a "YourAdChoices" link. Interviews with their representatives demonstrated that evaluated member companies understand it is key for consumers to be able to quickly and easily locate information regarding these companies' IBA and CAA activities.

Pass-On Notice

Although the NAI's self-regulatory program applies only to its members, NAI members can in turn help ensure, through contractual requirements with consumer-facing website and application publishers, that consumers have access to information about IBA and CAA data collection and use respectively (Code § II.B.3.; App Code § II.B.3.). These contractual notice

provisions are important as they help ensure consumers are provided with notice at the point of data collection, including in instances where the ad icon or other in-ad notice is not available because IBA or CAA-based ads are not present on a given site or in an application. This would be the case where a retailer site or app is engaged in Retargeting, for example.[24] Based on a review of evaluated member companies' sample partner contracts, the NAI found that evaluated member companies overwhelmingly included such contractual requirements when working directly with website and application publishers.[25]

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

The NAI found that many evaluated member companies continued to conduct due diligence on websites and applications where they sought to conduct IBA and CAA activities when initiating a relationship with those partners. Some evaluated member companies trained their sales teams to evaluate such notice when onboarding new partners, while other member companies did not do business with partners unwilling to include the notice.[26]

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

NAI staff provided guidelines for procedures to verify disclosures made by publisher partners in a manner that was feasible even for members with limited resources. In addition, the NAI provides its members with a static web page and a shareable document as a reference point for these pass-on notice requirements, making it easier for member companies to explain this requirement to partners.

Enhanced Notice Requirement

The Codes require that members provide, and support the provision of, notice in or around advertisements informed by IBA and CAA. This requirement provides just-in-time notice by NAI members to consumers, offering yet another means by which consumers can be informed of members' IBA and CAA activities, and the choices available to them. In 2016, NAI members continued to lead industry efforts to provide real-time notice and choice to consumers in and around the ads delivered to them by serving a form of enhanced notice, such as the YourAdChoices icon which is served at a rate of one trillion times per month.[27] Those evaluated member companies that offer technology platforms, and only facilitate the collection of data by their clients for IBA, provided their clients with the ability to include this notice on their advertisements through the platform settings.

Health Transparency

NAI members are required to publicly disclose the standard interest segments they use for IBA and CAA that are based on health-related information (Code § II.B.2.; App Code § II.B.2.). In this context, "standard segments" are those profiles based on health-related information that are pre-packaged and offered for IBA or CAA purposes by a member. Standard segments do not include those profiles offered to advertisers that are created or customized on a request basis for a specific advertiser or advertising campaign. This requirement calls for members to disclose not only sensitive health segments (such as an inference that a consumer may be interested in products or treatments for cancer, mental health conditions, or sexually transmitted diseases, among others), but also inferred interests in non-sensitive topics, such as skin care, diet, or fitness. Because the relative sensitivity of a health condition or treatment is often subjective, the goal behind this broad disclosure requirement is to allow consumers to make their own educated decisions about whether to opt out of the collection and use of data for IBA and CAA by a specific member company, dependent on the type of health-related targeting the company engages in. This disclosure requirement continues to be separate and distinct from the Opt-In Consent[28] requirement for IBA and CAA uses of sensitive health data discussed later in this report.

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

As business models are constantly in flux, NAI staff found that many evaluated member companies no longer offer a taxonomy of standard interest segments.[29] Instead, many evaluated member companies offer custom, non-sensitive health segments for individual advertising campaigns. Understanding that an exhaustive list of customized segments would be impossible, NAI staff continues to encourage those members to publicly provide representative samples of such customized segments to better educate the public about their activities.

USER CONTROL

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

Presence of Opt-Out Mechanisms

2016 marked the first annual compliance review of evaluated member companies' Opt-Out Mechanisms for Cross-App Advertising.

NAI members are required to provide consumers with the ability to opt out of the collection and use of Non-PII[30] for IBA and CAA purposes, including Retargeting. Member companies must provide access to Opt-Out Mechanisms for IBA and CAA on the member's website, in addition to an Opt-Out Mechanism for IBA on the NAI website (Code § II.C.1.a.). In 2016 the NAI independently confirmed that evaluated member companies conformed to these requirements.

2016 marked the first annual compliance review of evaluated member companies' Opt-Out Mechanisms for CAA. All reviewed member companies attested to honoring platform-provided choice mechanisms,[31] third-party choice mechanisms,[32] or both. Thus, all evaluated member companies provided an Opt-Out Mechanism for CAA. However, NAI staff's conclusion that some member companies needed to improve their mobile-specific disclosures also extended to descriptions of, and instructions relating to, CAA Opt-Out Mechanisms.[33] Consequently, NAI staff worked with member companies to help provide more thorough opt-out instructions, and will be monitoring these disclosures closely in 2017 to help ensure improvement in this important area.

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

HONORING OPT-OUT MECHANISMS

NAI monitoring tools checked for the persistence of opt-out cookies over 370,000 times.

The Codes require that members honor the user's choice as to the particular browser when opted-out of IBA and as to a particular device when opted-out of CAA (Code § II.C.2.; App Code § II.C.2.). A member must stop the collection and use of data for IBA or CAA while an opt-out preference is set and stored on a given browser or device, respectively.[34]

In 2016 NAI staff took multiple steps to help evaluated member companies confirm their compliance with these requirements. Evaluated member companies filled out a detailed compliance questionnaire regarding the functionalities of their Opt-Out Mechanisms, including listing the types of technologies they used for IBA and CAA. All evaluated member companies that continued to set cookies with unique identifiers while an opt out was present on a browser confirmed during the annual compliance review interviews that such use was for non-IBA purposes only, such as for analytics, frequency capping, and attribution, as permitted by the Code.

The questionnaire responses, combined with manual testing by NAI staff, indicated that evaluated member companies stopped using data for IBA purposes in the presence of an opt-out cookie. While NAI staff is able to examine app-based data flows with its monitoring tools, the monitoring software does not yet possess the same functionality as it does for browser-based, client-side opt outs. Nonetheless, questionnaire responses and interviews backed by member-signed attestations indicated that evaluated member companies ceased collecting data for CAA when receiving an opt-out signal.

In a review of the expiration dates of opt-out cookies set by evaluated member companies, NAI staff noted that these cookies had expiration dates at least five years into the future, as required by the NAI, and often were set to last considerably longer than this mandated minimum.[35]

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

Technologies Used for IBA

Though the Code is intended to be technology-neutral with respect to the technologies that can be used for IBA,[36] NAI members have historically used HTTP cookies for this purpose. However, member companies may also use non-cookie technologies for IBA purposes, so long as they do so in compliance with the Code, including provisions regarding notice and choice (Code § II.C.3.).

The NAI worked with its members in 2015 to develop and publish the *NAI Guidance on the Use of Non-Cookie Technologies for Interest-Based Advertising*.[37] This guidance clarifies how Code requirements may be met when member companies use non-cookie technologies for IBA and ADR.

More specifically, this guidance articulates the NAI's requirements for transparency, notice, control and accountability when member companies use non-cookie technologies. To illustrate, such companies must add to their privacy disclosures a statement that non-cookie technologies are being used for IBA and/or ADR. Furthermore, member companies must work with website publishers to include these disclosures in line with the NAI's pass-on notice requirements. To aid member companies, this guidance includes examples of language that can be passed on to website publishers. Additionally, member companies that use non-cookie technologies must increase transparency around their use of these technologies. To help facilitate this transparency, the NAI tested a new consumer opt-out page in 2016 that allows member companies to provide notice of their use of non-cookie technologies and to provide consumers a more robust choice mechanism when non-cookie technologies are used. This page ultimately launched to the public in early 2017 in a joint effort with the DAA.

Where evaluated member companies notified the NAI regarding the use of non-cookie technologies, NAI staff worked with evaluated member companies in 2016 to help ensure their privacy disclosures reflected the use of these additional technologies (Code § II.B.1.d.).

In a process started the prior year, expanded technical reviews in 2016 resulted in data collection reports which provided aggregated summaries of members' data collection activities not easily visible using standard browser tools. Supplemented by the compliance questionnaires and telephone interviews, NAI staff endeavored to independently confirm when non-cookie technologies were used by evaluated member companies.[38] The NAI's data collection reports helped staff review 42,469 data elements, including cookies, URL queries, headers, Javascript files, pixel tags, and various markup languages—nearly twice as many as last year's review, which itself was expanded from prior assessments.

The 2016 compliance review process and the NAI's technical reviews indicate that those members using non-cookie technologies for IBA or ADR in 2016 did so in a manner consistent with the Code and with the *NAI Guidance on the Use of Non-Cookie Technologies for Interest-Based Advertising*. Those members provided the required notice, transparency, and control under the Guidance.

OPT-IN CONSENT

The Codes require member companies to obtain Opt-In Consent for:

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

Merger

During the 2016 annual compliance review the vast majority of evaluated member companies reported that they did not merge PII with Non-PII for IBA or CAA purposes. Many evaluated member companies, in fact, continued to employ mechanisms to help ensure that they did not inadvertently collect or receive PII for IBA purposes. They often imposed contractual restrictions forbidding their data providers or partners from passing PII to them, and some reinforced these contractual requirements through technical controls that immediately discarded PII unintentionally passed to the member company for IBA or CAA purposes.

One evaluated member company indicated that it may merge PII with Non-PII for IBA and CAA purposes. This company has a first-party relationship with users and is able to obtain Opt-In Consent, or provide robust notice combined with an Opt-Out Mechanism, as required by the Codes for such merger.[39] NAI staff reviewed the notice and choice mechanisms offered by this company and found that they met the relevant requirements in the Codes.

Precise Location Data

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

To help NAI members navigate the requirements for the use of these data points the NAI provides *Guidance on Determining Whether Location is Imprecise*.[40] This guidance is intended to assist NAI members in the determination of whether the data they are using for IBA or CAA must be accompanied by Opt-In Consent, and encourages members to render location data imprecise before storage by eliminating data points or truncating decimal points from coordinates. This guidance document suggests that member companies consider four factors when determining whether location data is imprecise, including the area of the identified location the population density of that area, the accuracy of the data, and the precision of the location data's timestamp. Ultimately the goal of this guidance is to protect consumer privacy, by providing a disincentive for the storage of data that could be used to determine the actual physical location of a device, while allowing for the use of broader location-based data, such as whether consumers are likely to visit coffee shops, or sit-down restaurants.

This was the first annual compliance review to include data collection and use through mobile applications. Not surprisingly, NAI staff found significantly more evaluated member companies engaged in the collection or use of Precise Location Data for IBA and CAA than had been the case when reviews were focused solely on data collected from websites. These evaluated member companies attested to NAI staff that they received reasonable assurances[41] that their publishing partners obtained Opt-In Consent for the IBA and CAA uses of the Precise Location Data (Code § II.C.1.d.; App Code § II.C.1.d.).

Sensitive Data

Sensitive Data is defined to include specific types of PII that are sensitive in nature, as well as certain Non-PII related to health information and sexual orientation (Code § I.H.; App Code § I.H.). NAI staff found that evaluated member companies did not use Sensitive Data for IBA or CAA purposes in 2016 and continued to have a uniformly high awareness of the requirements for the use of Sensitive Data for IBA and CAA. Consequently, evaluated member companies maintained the protections they had in place to ensure that Sensitive Data was not used for IBA and CAA.

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

Further, from the inception of the Privacy Disclosure Scanner, NAI staff has been able to regularly review changes to the health segments publicly disclosed by evaluated member companies, as required by the health transparency requirement of the Codes. This enabled staff to work with members to help determine if a member added a segment that could be deemed sensitive per the analysis of relevant factors set forth in the commentary of the Code. This was rarely necessary, however, as NAI member companies frequently reached out to NAI staff for help in weighing whether certain segments could be considered sensitive under the Codes.

Sexual Orientation

The Codes prohibit member companies from using data collected across unaffiliated web domains to associate a browser or device with IBA or CAA 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 or CAA.

USE LIMITATIONS

Children

The Codes require that members obtain verifiable parental consent for the creation of IBA and CAA segments specifically targeting children under 13 years of age (Code § II.D.1.; App Code § II.D.1.). During the 2016 annual review, all evaluated member companies indicated awareness of the sensitivity of data related to children for IBA and CAA, and advised the NAI that they had processes, policies, and procedures in place to prevent creation of IBA and CAA segments specifically targeted at children under 13.[42]

Eligibility

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

Aside from the expressly forbidden eligibility uses of IBA, CAA, and ADR data detailed above, in 2016 NAI staff once again used the compliance reviews as an opportunity to educate its members about the need to avoid other potentially problematic uses of IBA, CAA, and ADR data, such as for tenancy or education admissions eligibility. Based on discussions with evaluated member companies NAI staff concluded that members did not use, and were not aware of any partner use of, IBA and ADR data for these purposes.

Material Changes

The Codes require that members who make a material change to their IBA or CAA data collection and use policies and practices obtain Opt-In Consent before applying such change to previously collected data (Code § II.D.3.; App Code § II.D.3.). In 2016 NAI staff questioned evaluated member companies and discussed changes to business models to help identify any potential material changes invoking this requirement, and evaluated member companies also attested to their compliance with this provision.

TRANSFER RESTRICTIONS

During the 2016 annual compliance review, evaluated member companies attested to their compliance with the obligation to contractually require any partners to whom they provide Non-PII, to be merged with PII data possessed by that partner for IBA or CAA, to adhere to the applicable provisions of the Codes (Code § II.E.1.; App 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 or applications owned or operated by different entities, to not attempt to merge such data with PII held by the receiving party or to re-identify the individual for IBA or CAA purposes without obtaining Opt-In Consent (Code § II.E.2.; App Code § II.E.2.).

DATA ACCESS, QUALITY, SECURITY, AND RETENTION

Reasonable Access to PII

As discussed, the NAI staff confirmed with a vast majority of evaluated member companies that they did not collect PII for IBA or CAA purposes. The evaluated member company that used PII for IBA and CAA purposes provided reasonable access to this data[43] (as required by the Codes) through its consumer-facing portals.

Reliable Sources

Evaluated member companies attested, and explained in interviews, that they obtain data from reliable sources (Code § II.F.2.; App Code § II.F.2.) that collect data while providing appropriate levels of notice and choice to users. Evaluated member companies overwhelmingly reported conducting appropriate due diligence on data sources to help ensure their reliability, including reviewing the potential partners' business practices, particularly when those partners were not members of the NAI and thus could not be counted on to have undergone the same compliance review. In rare instances where members did not fully understand the Codes' obligations regarding data quality, NAI staff offered suggestions and best practices to help them develop due diligence processes in regard to data partners.

Reasonable Security

The Codes impose a requirement designed to help ensure that data used for IBA, CAA, and ADR activities is adequately secured. Evaluated member companies attested that they complied with this obligation to reasonably secure data (Code § II.F.3.; App Code § II.F.3.).[44]

Retention

During the 2016 annual compliance review, NAI staff discussed with evaluated member companies the Codes' requirement to retain data only as long as necessary for a legitimate business purpose (Code § II.F.4.; App Code § II.F.4.). Evaluated member companies were required to attest to the longest duration of IBA, CAA, and ADR data storage. Member companies are also required to publicly disclose the period for which they retain such data (Code § II.B.1.e.; App Code § II.B.1.e.).

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

ACCOUNTABILITY

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

SANCTIONS

A thorough compliance assessment process and the availability of strong sanctions combine to form the keystone of the NAI self-regulatory program. The NAI also firmly believes that identifying problems early, and giving member companies an opportunity to resolve minor issues, allows members to address potential issues before they can affect the broader population and therefore become material, thus necessitating stronger sanctions. This approach fosters an environment of mutual trust between the NAI and its members, and ultimately results in enhanced privacy protection for consumers as members become more open about potential shortcomings and more willing to voluntarily participate in self-regulatory efforts.

NAI staff investigates private and public allegations of noncompliance. Staff also searches for evidence of noncompliance in the reports generated by the NAI's automated monitoring tools. In the event that NAI staff finds, during any of the compliance processes, that a member company may have materially violated the Codes, the matter may be referred to the Compliance Committee of the Board of Directors with a recommendation for sanctions.[45] Should the NAI Board determine that a member has violated the Codes, the NAI may impose sanctions, including suspension or revocation of

membership. The NAI may ultimately refer the matter to the FTC if a member company refuses to comply. The NAI may also publicly name a company in this compliance report, and/or elsewhere as needed, when the NAI determines that the member engaged in a violation of the Codes.

In 2016 NAI staff conducted several investigations of potential violations of the Codes. Ultimately NAI staff found that the member companies in question did not materially violate the Codes and consequently sanctions procedures were not appropriate.

As was the case during prior annual compliance reviews, in 2016 NAI staff found a number of lesser violations of the Codes by some member companies. These member companies willingly resolved such issues raised by NAI staff. Often member companies implemented additional measures voluntarily to reduce the likelihood of future noncompliance. Based on its historical approach to minor infractions, typically caused by misunderstandings or technical glitches, NAI staff worked with members to resolve issues before they become material violations of the Codes. As in the past, this approach helped fix issues expeditiously, while reserving sanctions for material violations of the Codes and helping to ensure the vitality of the ecosystem.

SUMMARY OF FINDINGS

NAI staff found that in 2016 evaluated member companies complied with the Codes, and to the extent that any violations were identified, they were not material. Evaluated member companies demonstrated that they remain vigorously committed to the NAI's self-regulatory framework. Representatives from evaluated member companies welcomed feedback and best-practice suggestions from NAI staff, demonstrating their commitment to providing and building top notch privacy protection programs.

CONCLUSION

This report demonstrates that the NAI continues to play an important role in promoting consumer privacy in the online advertising technology ecosystem, while working to provide up-to-date guidance to its member companies. In 2016 the NAI greatly expanded its scope when it began enforcement of the App Code, thus applying its high standards for data collection and use in targeted advertising to mobile devices. During this time the NAI finalized a fully reengineered consumer choice page and developed guidance on the linking of devices for targeted advertising purposes, efforts that ultimately came to fruition in early 2017. This report also establishes that through its annual compliance review process, the NAI and its staff closely monitored the pulse of the advertising technology ecosystem, identifying industry trends as well as associated problems and opportunities for improvement.

The review process manifests NAI member companies' determination to protect consumer privacy. These companies voluntarily subject themselves to a time-consuming and extensive review every year, and in doing so they demonstrate their commitment to some of the strongest self-regulatory principles in the industry.

The NAI is satisfied with the efforts of its members to comply with the Codes and other NAI guidance. Nonetheless, the NAI recognizes room for improvement in several areas. 2017 will mark the launch of the NAI's updated consumer choice page, providing additional transparency and functionality in a wider variety of browser settings, as well as the publication and enforcement of the NAI's guidance on the use of cross-device technology for targeted advertising. A new public service campaign will alert consumers about these initiatives and the additional materials available through the NAI. The NAI plans to continue work on synthesizing its Code and App Code into one document in order to make NAI requirements easier to grasp for the public, while further expanding coverage to emerging digital advertising products and technologies. The NAI will also advance work with its members and with industry stakeholders to examine terminology.

As NAI members develop emerging technologies and business lines, the NAI is able to leverage its unique position in the advertising technology ecosystem to help ensure that industry self-regulatory efforts address the privacy challenges that may arise alongside these new products. In particular, the NAI uses its member and staff expertise and technical know-how to adapt proven privacy standards to new technologies. The digital advertising space moves at a rapid pace and the NAI is up to the challenge of keeping its policies and methods fluid as we explore the role of self-regulation in fields such as wearable devices, smart televisions, appliances, and automobiles.

NAI 2016

ENDNOTES

1 IBA is defined in the Code as "the collection of data across web domains owned or operated by different entities for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected" (Code § I.A.). Since 2015 the NAI has also applied the Code's IBA requirements to the practice of Retargeting, defined as "collecting data about a user's activity on one web domain for the purpose of delivering an advertisement based on that data on a different, unaffiliated web domain" (Code § I.C.).

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

4 The App Code defines CAA as "the collection of data through applications owned or operated by different entities on a particular device for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected" (App Code § I.A.).

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

6 A 2014 study shows that offering relevant advertising to visitors benefits smaller websites, providing essential revenue to the "long tail" of web content. http://www.aboutads.info/resource/fullvalueinfostudy.pdf.

7 The 2015 Update to the NAI Code of Conduct can be found at: https://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf.

8 The 2015 Update to the NAI Mobile Application Code can be found at http://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf.

9 Federal Trade Commission, *Fall Technology Series: Smart TV*, https://www.ftc.gov/system/files/documents/public_events/942763/smarttv_agenda_12_7.pdf.

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

11 The NAI urges applicants and member companies to consult with their own technology and legal experts when reviewing the privacy implications of products and business plans.

12 The following nineteen companies went through the new member application process and became NAI members in 2016: Adobe, Anomaly, Appreciate, Arbor.IO, Audience Trust, Beeswax, Choozle, Clearstream, Cuebiq, Eyeota, Factual, Ninth Decimal, Numberly, PlaceIQ, Pulpo, Retargetly, Signal, Skyhook, 12 Digit Media.

13 References to compliance with, and violations of, the Codes throughout this document are intended to address material compliance and violations. Examples of material violations include intentionally misleading users or NAI staff, refusing to institute NAI requirements, failure to cooperate with NAI staff, or failure to provide and honor consumer choice affecting a large number of users over an extended period of time. Members are typically allowed to resolve minor issues such as temporary technical glitches or inadvertent gaps in required disclosures before these issues become material.

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

15 The following companies were reviewed in 2015 but were not among evaluated member companies in 2016:

a. Ezakus, G4 Native, LiveRail, and Mode Media, were no longer engaged in IBA and CAA operations in the United States. These companies terminated their NAI memberships and did not complete the 2016 annual compliance review.

b. Pointroll was absorbed by NAI member Sizmek. Pointroll ceased independent operations and was therefore not evaluated independently of its parent company during the 2016 annual review process.

c. Adblade and Proclivity did not renew their NAI memberships.

16 *See supra*, note 12.

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

18 If a member has an agreement with a partner to collect data on the partner's site or app where it collects and uses data for IBA or CAA purposes, the member is obligated to require through its contractual provisions that the partner provide notice to the user and a link to an Opt-Out Mechanism (Code § II.B.3.; App Code § II.B.3.). This requirement is discussed more fully below.

19 NAI member companies comprise all of the Top 10, and 18 of the Top 25 Ad Networks according to the comScore Ad Focus Rankings (Desktop Only) as of April 2017, available at https://www.comscore.com/Insights/Rankings.

20 See https://www.internetalerts.org/.

21 See https://votinginfoproject.org.

22 Members are not required to disclose the technologies they use for IBA, CAA, 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, CAA, and/or ADR.

23 As described above, with the Privacy Disclosures Monitoring Tool, NAI monitors member privacy disclosures to ensure that members do not inadvertently remove language required by the Codes.

24 *See* the discussion regarding the "Enhanced Notice Requirement" below.

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

26 The NAI's compliance reviews are limited to the practices and disclosures of its members.

27 Because of continuing technical challenges with providing enhanced notice in specific formats of video advertisements, the NAI is not enforcing this requirement in video advertisements at this time. The NAI will issue a formal compliance notice before enforcement of this requirement is implemented once the technological challenges are overcome.

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

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

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

31 *See e.g.* Opt out of interest-based ads in the App Store and Apple News, https://support.apple.com/en-us/HT202074.

32 *See e.g.* http://youradchoices.com/appchoices.

33 *See supra* p. 19.

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

35 *See* http://www.networkadvertising.org/faq/#n17.

36 *See* the Introduction and Commentary to Code.

37 *See* http://www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf.

38 The data collection report is produced by intercepting web packets from test browsers or devices and then creating an aggregate report of a variety of supported data elements, including cookies, custom header fields, JavaScript functions, image metadata, and mobile data collection methods. Together, these data points may help reveal when an active statistical identifier or client-side storage are in use.

39 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 and CAA purposes (prospective merger) (Code § II.C.1.b.; App Code § II.C.1.b.).

40 *See* http://www.networkadvertising.org/sites/default/files/NAI_ImpreciseLocation.pdf.

41 In 2016 the NAI adopted the Digital Advertising Alliance (DAA) standard of reasonable assurances of Opt-In Consent for Precise Location Data which provides a number of methods for third parties - like NAI member companies - to obtain Opt-In Consent, or reasonable assurances that a first party, such as a mobile application, has obtained such consent on their behalf. (Digital Advertising Alliance Mobile Guidance, § IV.B.2.).

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

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

44 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 Codes. 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 appropriate security measures for their specific circumstances.

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

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

NAI
Network Advertising Initiative