

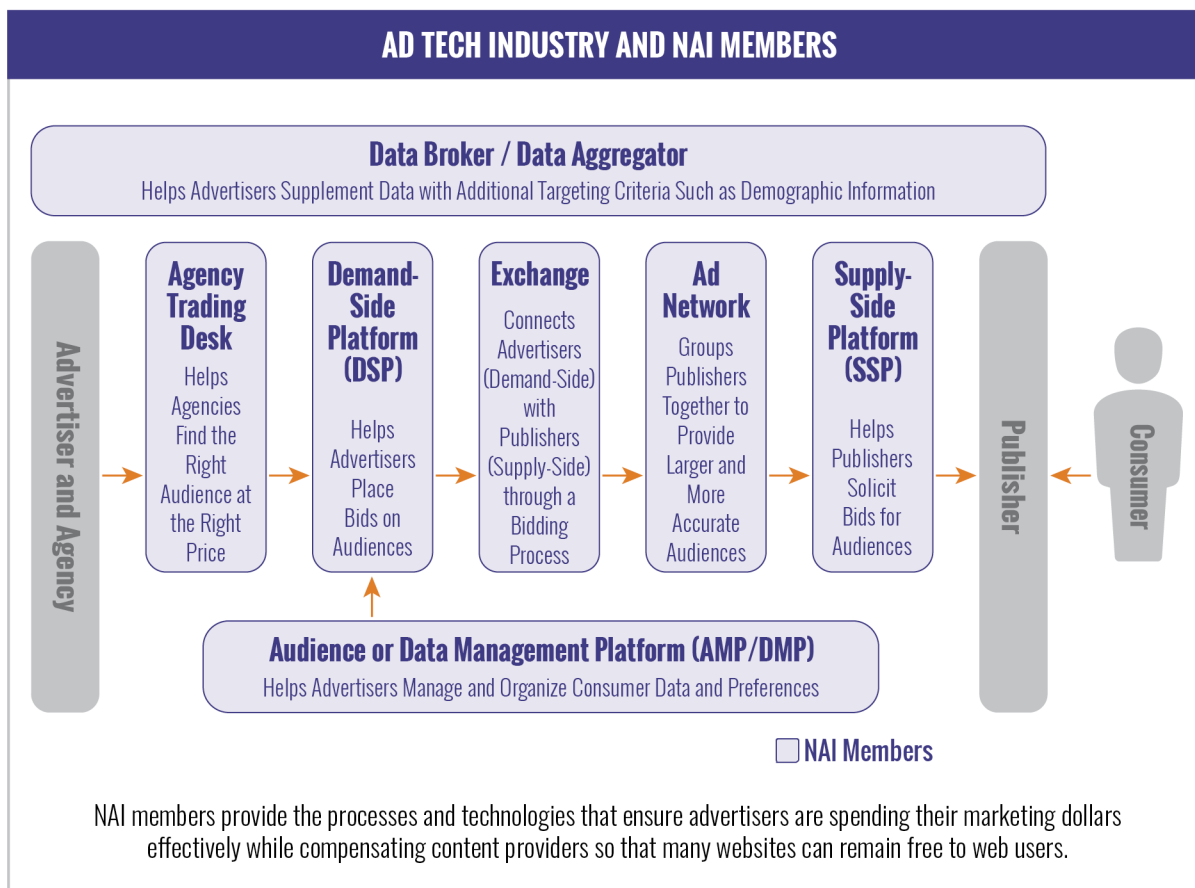
2017 ANNUAL
COMPLIANCE
REPORT

TABLE OF CONTENTS

2	Introduction
4	2017: The Year in Review
7	The NAI Compliance Program
17	2017 Annual Review Findings
34	Conclusion
38	Endnotes

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 105 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. This process also results in periodic updates to NAI Codes and guidance documents to keep pace with evolving technologies and digital advertising business models. **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 2017 as well as staff’s findings from the 2017 compliance review. During the 2017 compliance period, NAI staff reviewed members’ compliance with the Code⁷ and the App Code⁸ (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 that continues to be highly relevant amidst marketplace changes.

2017: THE YEAR IN REVIEW

The NAI's self-regulatory program continues to develop and progress along with the advertising technology ecosystem and the privacy field more broadly. Each year the NAI sets forth its goals for the following year, and for 2017 the NAI pledged to: (1) launch a new consumer choice page, providing additional functionality and transparency; (2) publish guidance on the use of cross-device technology; (3) merge its Code and App Code into an updated document; (4) work with members and industry stakeholders to reexamine terminology in the Code; (5) continue improvement of its technical monitoring suite; and (6) examine the role of self-regulation in the connected television space.

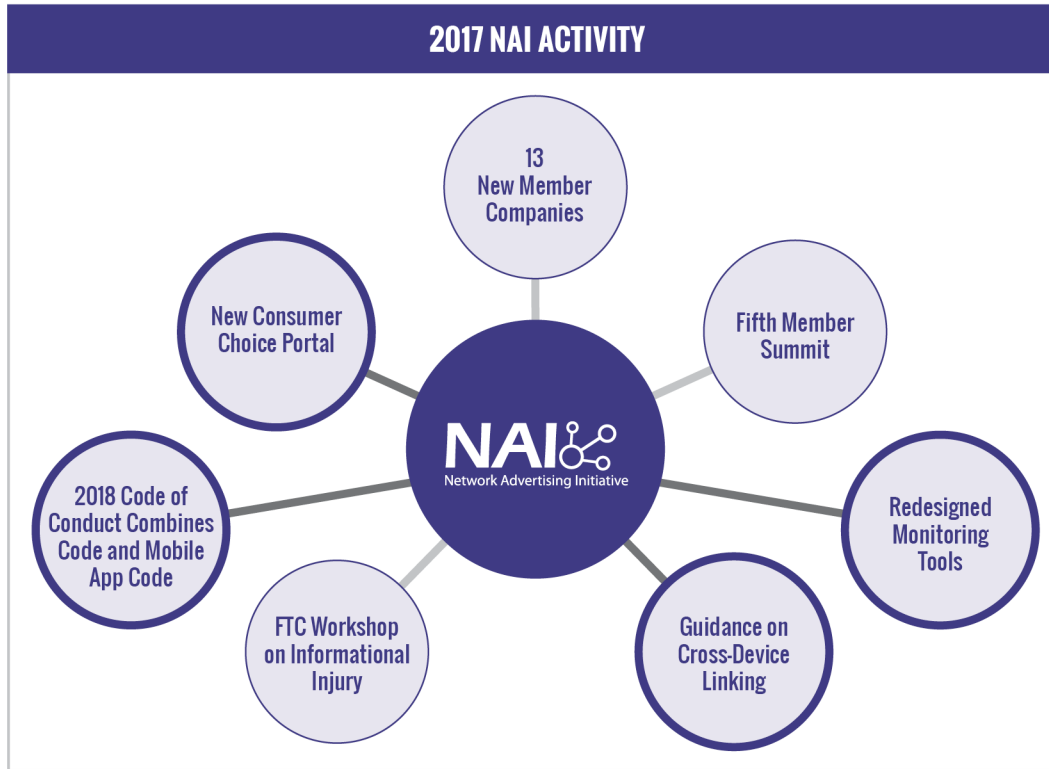
In 2017, 13 new member companies were approved by the NAI Board of Directors.

The NAI launched its new and revamped consumer choice tool in April of 2017, the culmination of more than a year of work and research intended to provide more transparency regarding non-cookie technologies and additional controls for users with browsers that block third-party cookies by default. 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 NAI published its Guidance for NAI Members: Cross-Device Linking⁹ in May of 2017, beginning enforcement of the guidance document on June 19, 2017. This document updated 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.

NAI staff and its Board of Directors combined the Code and App Code into a single document, the 2018 NAI Code of Conduct (2018 Code), published in November of 2017, and enforced as of January 1, 2018.¹⁰ This document not only combines previously separate guidance regarding web-based and app-based data collection and use for digital advertising, but also includes revised terminology to better reflect the potential identifiability of various data types. As the 2018 Code was not in force during the 2017 NAI compliance review, this document only references requirements and terminology present in the Code and App Code. The upcoming 2018 compliance review will be conducted using the 2018 Code.

Throughout 2017, NAI staff worked on a complete overhaul of its technical monitoring tools to provide more consistent results and dramatically improved functionality while keeping up with developments in data-collection technologies. This project continues to be a work in progress but has already led to a more dependable view of members' activities.



NAI staff worked with members and other industry stakeholders to monitor technical and policy developments in the connected television space. The information gleaned from this process is being incorporated into draft guidance for NAI members, which the NAI plans to share with stakeholders and regulators in 2018, ahead of potential publication.

Also in 2017, the NAI hosted its fifth annual Summit, bringing this one-of-a-kind industry event back to New York City. 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 2017 Summit featured a fireside chat with Federal Trade Commission (FTC) Commissioner, Terrell McSweeney, and also included timely discussions about “fake news,” regulatory developments in Europe, and other relevant topics which inform NAI members’ behavior in the marketplace.

NAI staff worked closely with staff at the FTC to better understand issues relating to informational injuries. This involvement included the FTC’s Informational Injury Workshop in December of 2017, where NAI CEO, Leigh Freund, participated in a panel weighing how businesses evaluate the risks associated with digital data collection.¹¹

Thirteen new members joined the NAI in 2017. 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. Compliance efforts begin even before a company becomes a member. 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 NAI 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, an 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 based on the application materials, or assessment of business practices that may be inconsistent with the Codes.

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 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, for others, the initial qualification assessment can often be a months-long process, with the NAI providing guidance and suggestions about compliance along the way. As a result of the NAI application review process, many applicants make substantial revisions to their public privacy disclosures in order to provide the full level of notice required by the Codes. Typically, NAI staff provides technical guidance to help an applicant develop an Opt-Out Mechanism¹² that is capable of meeting the Codes' requirements and to ensure compatibility 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.¹³

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 2017, thirteen companies¹⁴ completed the application process and were approved for membership by the Board.

At the close of the 2017 compliance review period, the NAI Board consisted of:

Douglas Miller, Chairman, NAI Board of Directors; *Vice President and Global Privacy Leader, Oath Inc.*

Ted Lazarus, Vice-Chairman, NAI Board of Directors; *Director, Legal, Google*

Estelle Werth, Secretary, NAI Board of Directors; *Vice President, Global Privacy Officer, Criteo*

Julia Shullman, Treasurer, NAI Board of Directors; *Senior Director, Deputy General Counsel, Commercial & Privacy, AppNexus*

Jason Bier, *EVP, General Counsel & Chief Privacy Officer, Engine Media*

Andy Dale, *Vice President, Legal, and Data Protection Officer, DataXu*

Brooks Dobbs, *Chief Privacy Officer, KBMGroup*

Ken Dreifach, *Shareholder, Zwillgen, on behalf of AdRoll*

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

Ghita Harris-Newton, *Chief Privacy Officer, Deputy General Counsel, Quantcast*

Brad Kulick, *Senior Director of Privacy, Advertising & Analytics Privacy, Yahoo!*

Ari Levenfeld, *Chief Privacy Officer, Sizmek*

Alice Lincoln, *Vice President of Data Policy & Governance, MediaMath*

Noga Rosenthal, *Chief Privacy Officer, Conversant/Epsilon*

Stability improvements to the NAI monitoring tools allowed staff to perform scans twice as often as in the past.

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 compliance¹⁵ so long as they maintain their membership. One way the NAI helps facilitate this process, even in between the annual NAI compliance reviews, is through its automated monitoring suite which includes an Opt-Out Scanner and Privacy Disclosures Scanner that allow staff to flag potential issues for review or investigation. **The NAI monitoring suite is under continuous development** and was effectively rebuilt in 2017 to provide improved stability and functionality.

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 potential 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. Once an issue is flagged through the monitoring tools, NAI staff promptly reviews the situation. Upon further review, NAI staff typically confirmed that these flags did not actually involve 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 might have resulted in violations of the Codes if left unaddressed. For example, several NAI members were acquired by or merged with other companies, resulting in changes to their privacy disclosures. In other cases, members' privacy policy links were accidentally removed, or were not moved to new domains during a rebrand. Such issues were generally spotted by NAI staff very rapidly and resolved by member companies shortly after notification. None of these instances were considered to rise to the level of material noncompliance with the Code because the underlying issues were resolved quickly, were found to be unintentional, and affected a limited number of consumers. Additionally, where applicable, NAI staff suggested methods through which members could prevent such issues from recurring in the future.

Web-based Opt-Out Testing

The NAI administers ongoing reviews of member opt outs through routine manual checks of the NAI's opt-out page followed by more in-depth analysis relying on technical tools. An NAI staff member routinely verifies that the NAI opt-out page continues to function as expected, and follows up with an in-depth network analysis and server-side inspection of each NAI member to investigate any anomalies. Although problems were rare, the majority of issues investigated in 2017 were the result of member company HTTP headers that may have impacted opt-out functionality in specific browsers. Each member company, when integrating for the first time with the NAI opt-out page, has its own configuration checked and tested by NAI staff, which prevents many issues prior to live deployment.

During 2017 NAI staff worked diligently to improve the stability and functionality of its Opt-Out Scanner to provide a more comprehensive and clearer picture of online traffic. 2017 development efforts centered on providing even more reliable and robust coverage of opt-out functionality and more rapid discovery of any potential errors.

Additionally, the NAI monitors and reads consumer emails received regarding specific functionality issues that may be difficult to identify with in-house testing, such as temporary malfunctions on load-balancing servers that affect only certain regions of the United States.

This multi-faceted approach aims to promptly 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 noncompliance with the Codes.

Privacy Disclosures Scanner

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 and broken links or non-conforming opt-out mechanisms. NAI staff works with members to promptly address such inconsistencies.

The Privacy Disclosures Scanner helps 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 allows NAI staff to help members evaluate how existing requirements

In 2017 the NAI Privacy Disclosures Scanner monitored over 200 pages for changes that could affect member compliance with NAI disclosure requirements.

under 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 NAI staff, or members proactively disclosing a new product or technology. The 2017 compliance team relied on the Privacy Disclosures Scanner to focus more specifically on verifying that changes discussed with evaluated member companies were incorporated in their privacy disclosures.

2017 improvements to the NAI’s Privacy Disclosures Scanner allow NAI staff to tag sentences with specific categories of requirements related to the Codes. For example, NAI staff can label a certain disclosure sentence or paragraph as pertaining to Cross-Device Linking, or data retention, which is then added to an expanding library of several thousand samples. These annotations are blind-reviewed by separate NAI staff before inclusion in the database. This process has allowed

MONITORING TOOL PERFORMING A SAMPLE ANALYSIS OF A PRIVACY POLICY

Disclosure Categories

Active

- Available for Annotation Categorization
- Used in Predicting Expected Disclosures Per Company
- You can toggle these on/off anytime without losing data

Archived

- No longer expected of any company’s disclosures
- Archive when a category is no longer required, or has evolved enough that old examples should be nullified and re-evaluated.

Status	Name
Active	Non-Cookie Tech: Disclosure that this company uses non-cookie tech. This does not include IDFA, Google Ad-ID, as those are mobile identifiers. Non-Cookie tech means things like browser storage, setting or passive statistical identifiers.
Active	Third Party

Review Annotations

When you approve or reject, the annotation creator will see that it was approved or rejected. This is so that interns creating annotations have quick feedback. One At a Time View

Download all confirmed as .csv

#	Text	Category	Confirm	Reject
1	If you have an Apple device, you can opt out of interest-based advertising by updating to iOS 6.0 or higher, and setting Limit Ad Tracking to 'ON'. You can do this by clicking on Settings -> General -> About -> Advertising and toggling Limit Ad Tracking to 'ON'. Our system is designed to respect your choice and not use information to provide IBA when this setting is ON.	mobile_opt_out	Confirm	Reject
2	In Android devices with Google Play Services 4.0 and higher, companies can target advertising to mobile app users by using a unique identifier called the "Android Advertising Identifier." You can opt out of our IBA services by selecting "Opt out of Interest Based Ads." Our system is designed to respect your choice and not use information to provide IBA when this setting is ON.	mobile_opt_out	Confirm	Reject

Annotation Review Feedback

Recent annotations that were approved or rejected as a good example of the target category.

#	Text	Category	Confirmed By Reviewer?
1	OPT OUT To go directly to our opt out, click here.	web_based_opt_out	true
2	Data Security We have implemented reasonable security measures to protect the information in our care, both during transmission and once we receive it. This includes, but is not limited to, the use of firewalls and encryption. No method of transmission over the Internet, or method of electronic storage is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your information, we cannot guarantee its absolute security.	reasonable_security	true

In 2017, the NAI received over 4100 consumer queries through its website or via email.

the NAI to begin investigating basic machine learning models using the training data, which may permit the NAI to supplement manual disclosure reviews with automated analysis in the future. These efforts enabled NAI staff to double the amount of automated monitoring tests performed throughout the year.

In 2017, the NAI Privacy Disclosures Scanner captured over 4500 snapshots of privacy policies, monitoring over 200 pages. A manual review of all items flagged by the scanner led staff to discard approximately 1000 changes that were unrelated to the text of a privacy policy, but captured over 150 changes to disclosures that could have affected compliance.

To the extent member revisions to their privacy policies flagged by the Privacy Disclosures Scanner implicated disclosures that are required by the Codes, in NAI staff's judgement, each member addressed staff comments and made changes in their disclosures to comply with the NAI requirements within a reasonable time of NAI staff's notice to the member. As an example, NAI staff noted that in addition to providing its own opt out, and pointing users the NAI opt-out page, a member's disclosures also referenced a third-party Opt-Out Mechanism with which the company had not fully integrated. The member removed this reference from its disclosures within five hours of notification by NAI staff.

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 digital advertising. 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 compliance perspective.

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 2017, the NAI received and reviewed 4154 queries through its website, 174 contacts via telephone, and 2 letters via postal mail. NAI staff determined that, as in the past, a vast majority of the inquiries received did not pertain to issues within the scope of the NAI's mission. For example, many communications 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 15 percent of consumer inquiries were related to the NAI, the NAI Codes, or NAI member companies. The 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, ISP/workplace Internet filters or anti-virus software prevented opt-out cookies from being set on the consumer's browser, or temporary connectivity issues such as latency led to malfunctions. In three 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 summary, NAI staff determined that consumer communications received by the NAI in 2017, through postal mail, telephone, or the NAI 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 consumer 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 sections III.C.2 of the Code and App Code, which require 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 mechanisms. NAI staff sent test consumer queries to member companies with questions about privacy practices related to IBA or CAA. The questions were sent from personal email accounts and included new questions in follow-up tests to minimize the likelihood that evaluated member companies would know that the questions were sent by NAI staff.

In those instances where NAI staff initially did not receive a response, or received a response that was inadequate, the evaluated member company was 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 or staffing changes at the member company. Of the evaluated member companies, after follow-up and feedback from NAI staff when appropriate, 99% provided prompt and informative responses. 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 Allegations and Complaints

In addition to the NAI's own monitoring and research, **NAI staff also scrutinizes a variety of other sources for potential instances of member noncompliance, including published articles, public allegations by privacy advocates, complaints to the NAI by third parties or other NAI members, and investigations by other regulatory bodies.** In 2017, NAI staff conducted one investigation based on public allegations of potential non-compliance with the Codes.¹⁶

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 2017 annual compliance review, NAI staff reviewed the 96 companies that were members from January 1 through December 31, 2017.¹⁷ This was the largest such review to date as the number of NAI members continues to increase. These members are referred to as “evaluated member companies” throughout this report. Those members that joined the NAI after January 1, 2017¹⁸ 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 2017 annual compliance review. Those members will be assessed again during the 2018 annual review process.¹⁹

Training

In 2017, the NAI provided a number of training and educational sessions for its members, including webinars and staff visits to member company offices.

The NAI launched its member education efforts in 2017 with a training webinar presented together with the DAA in January, designed to inform members about compliance with self-regulatory requirements related to Cross-Device Linking. This

presentation was intended to supplement the general training NAI staff provided members on individual policy issues throughout the year, and was followed by a second webinar on this same topic in June of 2017 to coincide with enforcement of the NAI’s Guidance on Cross-Device Linking.

In total, **the NAI held six all-member calls or webinars throughout 2017, including educational calls featuring other self-regulatory bodies or legal and technology experts.** NAI staff also made numerous visits to member company offices in order to provide in-person training and education regarding the Codes’ requirements and ongoing developments in the industry.

Written Questionnaire and Supporting Documentation

Evaluated member companies submitted written responses to the 2017 compliance questionnaire, which was substantially revised the prior year. The questionnaire required evaluated member companies to describe their business practices and policies in relation to the requirements of the Codes. In 2017 this questionnaire included, for the second year, questions related to 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

In 2017 the NAI reviewed 96 member companies. The largest such review to date.

and CAA activities;²⁰ 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 that their responses continued to be accurate to the best of the member's knowledge.

A minimum of two NAI staff members reviewed each evaluated member company's questionnaire responses and related materials to assess compliance with the Codes together with representations about business practices available from 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 sample advertising contracts.

Interviews

Following the review of questionnaire submissions and other supporting materials, at least two members of NAI staff interviewed representatives from every evaluated member company. 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 raised questions based on 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 and CAA.

Conducting interviews with all evaluated member companies provides the compliance team with additional in-depth insight into

each company's products, especially as new business models and technologies continue to emerge. This integrated view of the industry, resulting from direct engagement and regular contact with over 100 companies comprising a significant portion²¹ of the third-party advertising technology ecosystem, greatly increases the staff's ability to flag potential privacy issues to members and shapes NAI staff recommendations regarding future guidance and policies. The candor reflected in both compliance questionnaire and interview responses is only possible due to the mutual trust between NAI members and the organization.

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.

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. Evaluated member companies were also required to attest to the veracity of the information provided during the review process.

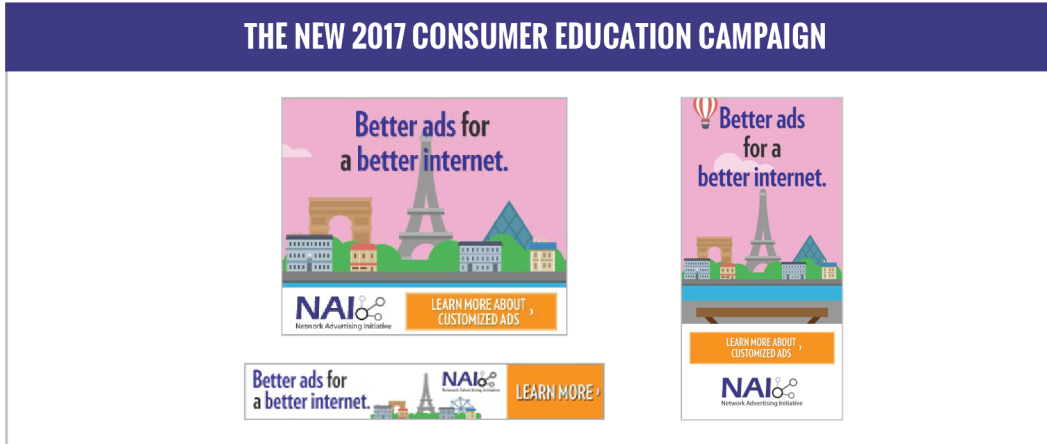
EVALUATED MEMBER COMPANIES

12DigitMedia	Defy (Break) Media	PlaceIQ
33Across	Drawbridge	Pubmatic
Accuen	Exelate	Pulpo
AcuityAds	Exponential/Tribal Fusion	PulsePoint
Adara	Eyeota	Quantcast
AddThis	eyeReturn	RadiumOne
Adobe	EyeView	Retargetly
AdRoll	Factual	RhythmOne
Aggregate Knowledge	Flashtalking	Rocketfuel
Anomaly	Gamut	Rubicon
AOL Advertising	Google	RUN
AppNexus	GumGum	ShareThis
Appreciate (formerly Triapodi)	I-Behavior (KBMG)	Signal
Arbor.IO (Formerly Pippio)	Ignition One	Simpli.fi
Atlas	Index Exchange (Casale)	Sizmek
Audience Trust	Innovid	Skyhook
BAM	Intent Media	Steelhouse
BazaarVoice	Kargo	Tagular
Beeswax	Krux	TapAd
BlueCava (Qualia)	Lotame	Trade Desk
BlueKai	Magnetic	TruEffect
BrightRoll (Yahoo)	Markit on Demand	TubeMogul
Choozle	Media.net	Turn
Clearstream/Engine Media	MediaForge	Undertone
Collective	MediaMath	Varick Media Management
Conversant	Microsoft	Viant
Criteo	MIG	Vibrant
Cross Pixel Media	Netseer	Videology
Cuebiq	Neustar	Xaxis
DataXu	NinthDecimal	Yahoo
Datonics	Numberly	Yieldmo
	OwnerIQ	YuMe
	Parrable	

2017 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 2017 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.

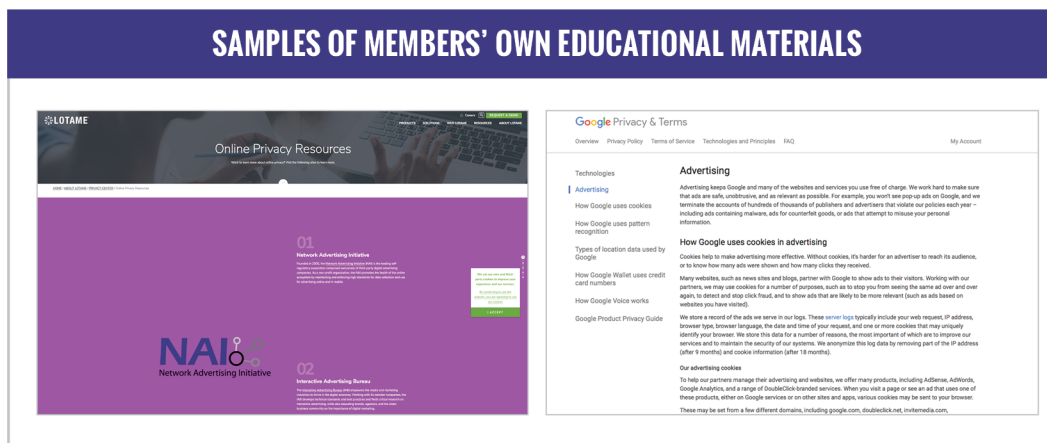
EDUCATION



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 provide a centralized education page that members may point to, implementing uniform terminology to help explain what can be a complex ad tech ecosystem to consumers. Accordingly, all members collectively educate consumers through the provision of the NAI website, which serves as a centralized portal for explanations of IBA, 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 2017, evaluated member companies met this obligation to collectively educate consumers about IBA, CAA, and available choices with respect to data collection for these purposes.

The NAI 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 launched this updated campaign in 2017 to educate consumers about the privacy implications of the latest developments in these technologies, and the most recent updates to NAI guidance. This new campaign ramped up in 2017, and will be heavily featured in 2018 thanks to promotion by member companies, to help increase consumer understanding of new technologies and products.

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),²² 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. Other NAI members participated in programs such as Data for Good,²³ providing the scientific community with access to limited data sets, which can in turn improve data models to enhance evacuation planning and execution in disaster areas or optimize city planning and transportation. 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 and CAA, 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 of data; a general description of the technologies used by members for IBA, CAA, and/or ADR activities;²⁴ a data retention statement; and an Opt-Out Mechanism. Finally, the Codes require members

The 2017 Compliance Review was the first to examine member compliance with requirements for Cross-Device Linking.

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.b.).

During the 2017 annual review, NAI staff assessed the privacy policies and other privacy-related disclosures of evaluated member companies in juxtaposition with the IBA, CAA, and ADR practices described in each company's annual interview, its corporate site, responses to the annual compliance review questionnaire, business model changes discovered through ongoing technical monitoring, and news articles.²⁵ 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 2017 to provide more information about data collection and use for CAA and ADR on mobile devices, as well as to better describe Cross-Device Linking practices.**

As this was the second year of required mobile-specific disclosures, NAI staff noted considerable improvement in such disclosures compared to 2016. Consistent with its commitment to continual improvement in consumer disclosures, the NAI will again work with members in 2018 to continue these efforts. 2017 was also the first year that NAI members were required to provide disclosures specific to Cross-Device Linking practices. Once more, NAI staff noted that while some companies presented model disclosures in this area, others still needed to provide this information in a clearer manner. NAI staff worked with evaluated member companies to help ensure that Cross-Device Linking disclosures are provided to users, and will continue working with members in 2018 to help further improve such disclosures.

Prominent Notice

In 2017 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 and CAA activities, and to exercise choice regarding IBA and CAA at their discretion.

As a result of ongoing educational efforts during prior compliance reviews, NAI staff found that at the time of their 2017 reviews, all evaluated member companies continued to provide an easy-to-find link to privacy disclosures in the footer or header of their websites. In some instances, NAI staff noted that links on members' home pages were moved or obscured by website redesigns. These issues were addressed by evaluated member companies within a reasonable timeframe after notification from NAI staff. As an example, NAI staff observed that a member company's privacy policy and opt-out links, in the footer of the company's site, could be difficult to identify due to the similarity in color between the text and background. The member company redesigned the footer and updated the color scheme within nine business days from notification.

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. Many evaluated member companies provided prominent privacy links outside of their site footers to make this information even more accessible to users. 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 (Code § II.B.3.; App Code § II.B.3.). These contractual notice provisions are important as they help provide consumers with notice at the point of data collection, including instances where an ad icon or other in-ad notice is not available because IBA or CAA-based ads are not present. This would be the case when a retailer site or app is engaged in Retargeting, for example.²⁶ A review of evaluated member companies’ sample partner contracts indicates that these companies generally included such contractual requirements while working directly with website and application publishers.²⁷

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 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, and some member companies did not do business with partners unwilling to include the requested notice.²⁸

Many evaluated member companies also perform random follow-up checks of their partners. A number of 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. At least one individual evaluated member company reported terminating relationships when 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 provided 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 (Code § II.B.5.; App Code § II.B.5.).

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 2017, 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 in nearly all targeted ads.**²⁹ Those evaluated member companies that offer technology platforms, and only facilitate the collection of data by their clients for IBA or CAA, provided their clients with the ability to include this notice on their advertisements through their own 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 segments based on interests in non-sensitive health topics, such as skin care, diet, or flu. 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, depending on the type

of health-related targeting the company engages in. This disclosure requirement continues to be separate and distinct from the Opt-In Consent³⁰ requirement for IBA and CAA uses of sensitive health data discussed elsewhere 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 of disclosures, NAI staff found that evaluated member companies continued to comply with this requirement 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 continues to improve each year, and that evaluated member companies continue to make more complete and accessible disclosures as a result of discussions with NAI staff.**

NAI staff found that many evaluated member companies no longer offer a taxonomy of standard interest segments.³¹ Instead, many evaluated member companies offer custom, non-sensitive health segments for individual advertising campaigns.

Understanding that an exhaustive list of one-off 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.

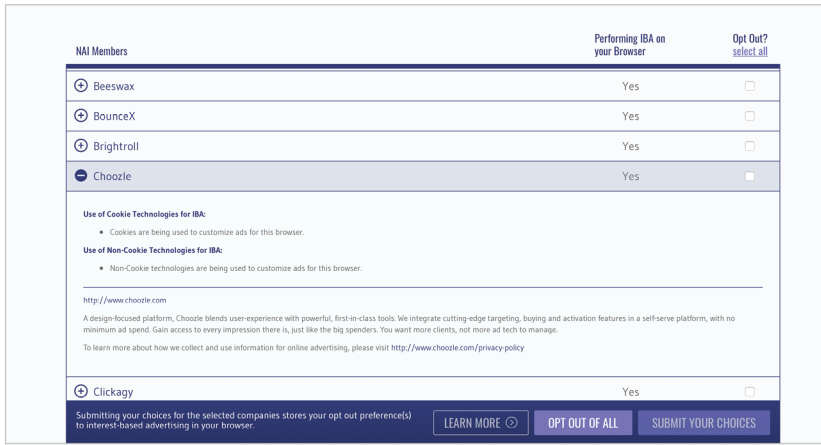
USER CONTROL

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 framework of the Codes 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

THE NAI COMPLETELY OVERHAULED ITS OPT-OUT PAGE IN 2017

The overhaul provides additional transparency and functionality in browsers that block third-party cookies by default.



NAI Members	Performing IBA on your Browser	Opt Out? select all
Beeswax	Yes	<input type="checkbox"/>
BounceX	Yes	<input type="checkbox"/>
Brightroll	Yes	<input type="checkbox"/>
Choozle	Yes	<input type="checkbox"/>

Use of Cookie Technologies for IBA:

- Cookies are being used to customize ads for this browser.

Use of Non-Cookie Technologies for IBA:

- Non-Cookie technologies are being used to customize ads for this browser.

<http://www.choozle.com>

A design-focused platform, Choozle blends user-experience with powerful, first-in-class tools. We integrate cutting-edge targeting, buying and activation features in a self-serve platform, with no minimum ad spend. Gain access to every impression there is, just like the big spenders. You want more clients, not more ad tech to manage.

To learn more about how we collect and use information for online advertising, please visit <http://www.choozle.com/privacy-policy>

Clickagy	Yes	<input type="checkbox"/>
----------	-----	--------------------------

Submitting your choices for the selected companies stores your opt out preference(s) to interest-based advertising in your browser.

[LEARN MORE](#) [OPT OUT OF ALL](#) [SUBMIT YOUR CHOICES](#)

NAI members are required to provide consumers with the ability to opt out of the collection and use of Non-PII³² 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.; App Code § II.C.1.a.). In 2017 the NAI independently confirmed that evaluated member companies conformed to these requirements.

2017 marked the second annual compliance review of evaluated member companies’ Opt-Out Mechanisms for CAA. NAI staff found that all reviewed member companies continued to receive and respect platform-provided choice mechanisms,³³ third-party choice mechanisms,³⁴

The NAI consumer choice tool, revamped for 2017, had over 12 Million visitors, up over 120% from 2016.

or both. Thus, all evaluated member companies provided an Opt-Out Mechanism for CAA.

Following its 2016 compliance review, the NAI noted that some member companies needed to improve their mobile-specific disclosures, including descriptions of, and instructions relating to, CAA Opt-Out Mechanisms (App Code § II.B.1.c.). Consequently, NAI staff continued to work with member companies to help provide more thorough opt-out instructions for mobile devices. As part of this effort, the NAI also developed a compendium of platform-provided choice mechanisms for mobile devices on its website,³⁵ allowing members an opportunity to point to these more detailed instructions as a means of meeting NAI requirements. While work remains to be done, the NAI is pleased with the progress its evaluated member companies have made in providing mobile-specific disclosures and Opt-Out Mechanisms, and staff will continue to work with members to continue improving these and other disclosures in 2018.

Through the use of the NAI's proprietary monitoring tools, staff noted on several occasions that different evaluated member companies' opt-out links, in their privacy policies or elsewhere on their sites, may not have been fully functional. These instances were exceedingly rare, and in nearly all cases 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). When such issues were spotted, evaluated member companies worked with NAI staff to quickly fix the broken links. Even when the potential issues were complex, such as those involving opt-out architecture, members worked diligently to resolve the matter as quickly as possible. During the course of one compliance review, NAI staff discovered that a member's Opt-Out Mechanism was experiencing difficulty in setting opt-out cookies from one of several necessary domains due to changes in some browsers' handling of HTTPS requests. Despite many other technical initiatives the company was involved in at the time, the issue was identified and resolved within ten business days from notification by NAI staff.

While the NAI's technical monitoring tools were able to flag the vast majority of potential problems, in two instances, during manual reviews of opt-out functionality in conjunction with the annual review process, NAI staff found that its automated monitoring technology had not flagged potential opt-out malfunctions on the centralized NAI opt-out page. As a result of these findings, the NAI significantly revised its automated testing procedures in 2017, and will continue to closely monitor opt-out functionality and the effectiveness of the NAI's monitoring technology in 2018.

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 identify broken or malfunctioning links in a prompt manner, thus minimizing the potential effect of technical failures on consumers.

HONORING OPT-OUT MECHANISMS

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.³⁶

In 2017 NAI staff took multiple steps to help evaluated member companies confirm their compliance with opt-out requirements. Evaluated member companies filled out a detailed compliance questionnaire regarding the functionality of their Opt-Out Mechanisms, including listing the types of technologies used for IBA and CAA. 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 that such use was for non-IBA purposes only, such as for analytics, frequency capping, and attribution, as permitted by the Codes.

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. Questionnaire responses and interviews backed by member-signed attestations indicated that evaluated member companies ceased collecting data for CAA when receiving an opt-out preference. In those instances where evaluated member companies did not directly collect data from a mobile device, but rather received such data through a third party or in an offline transfer, those evaluated member companies confirmed that they contractually require the data provider to either send opt-out flags along with the data or to refrain from sending such data altogether.

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.³⁷

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 nearly all 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,³⁸ 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.).

Because of unilateral moves by some browser manufacturers to block third-party cookies without any user input, the NAI worked with its members in 2015 to develop and publish Guidance on the Use of Non-Cookie Technologies for Interest-Based Advertising.³⁹ 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. 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 launched a new consumer opt-out page in April of 2017, in a joint effort with the DAA, allowing member companies to provide notice of their use of non-cookie technologies and to provide consumers a more robust choice mechanism when third-party cookies are blocked by default by a browser manufacturer.

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

The 2017 compliance review process indicates that the evaluated member companies that attested to the use of non-cookie technologies for IBA or ADR, 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 and Sensitive Data for IBA or CAA (Code §§ II.C.1.d-e.; App Code §§ II.C.1.d-e.); and
- for members who make 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 2017 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 or CAA 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.⁴⁰ 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.⁴¹ This guidance is intended to assist NAI members in the determination of whether the data being used for IBA or CAA must be accompanied by Opt-In Consent, and encourages members to render location data imprecise before its 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.

NAI staff found a number of evaluated member companies engaged in the collection or use of Precise Location Data for CAA across mobile applications. These evaluated member companies attested to NAI staff that they obtained Opt-In Consent directly from users, or received reasonable assurances⁴² that their publishing partners obtained Opt-In Consent for the CAA uses of the Precise Location Data on their behalf. (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 2017 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,⁴³ which outlines how the NAI will approach such issues, the NAI urges 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 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 on a preemptive basis for help in making such determinations.

Sexual Orientation

The Codes prohibit member companies from using data collected across unaffiliated web domains or applications to associate a browser or device with IBA or CAA segments 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 or CAA. Through the compliance review process, NAI staff found that no evaluated member companies created or used LGBT audience segments for IBA or CAA. One NAI member company, operating a technology platform, facilitated data collection on behalf of a popular LGBT dating service. This data was not directly used by the member company, as it operated only as a service provider for the company that had a first-party relationship with users. NAI staff confirmed that this dating service included disclosures in its terms of use to inform its customers that it could collect and share such data.

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 2017 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.

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 2017 annual review, all evaluated member companies indicated awareness of the sensitivity of data related to children for IBA and CAA, and all confirmed that they do not specifically target children under 13.** Additionally, several of the companies advised the NAI that they had processes, policies, and procedures in place to proactively prevent creation of IBA and CAA segments specifically targeting children under 13.⁴⁴

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.).

TRANSFER RESTRICTIONS

During the 2017 annual compliance review, evaluated member companies attested to their compliance with the obligation to contractually require any partners to whom they provide PII 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 to contractually require that all parties to whom they provide Non-PII, collected across unaffiliated 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 data⁴⁵ (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 obligations under the Codes 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. All evaluated member companies attested that they complied with this obligation to reasonably secure data. (Code § II.F.3.; App Code § II.F.3.).⁴⁶

Retention

During the 2017 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.a.v.).

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 explained these retention practices. In cases involving a retention deadline that reset each time a member company encountered a user, the NAI suggested appropriate disclosures to clarify the rolling nature of these timeframes. 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 internal training** (Code § III.A.2.; App Code § III.A.2.). Successful completion of the annual compliance review would not be possible without at least one individual at an evaluated member company to respond to the NAI questionnaire and conduct a telephone interview. However, NAI staff noted that on several occasions, turnover or reorganization led to temporary gaps in coverage of self-regulatory efforts at evaluated member companies. While these issues were quickly resolved once NAI staff notified the companies of their obligations under the Codes, as part of the compliance review, the NAI will focus more in 2018 on ensuring continuity of self-regulatory duties at member companies during personnel changes.

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.). In 2018 the NAI

Codes have been combined into a single document, streamlining requirements for member companies to disclose adherence to more than one NAI Code of Conduct.

INVESTIGATIONS AND SANCTIONS

A thorough initial qualification process, coupled with the annual compliance assessment process, use of technology to flag and address issues quickly, and the availability of strong sanctions should members fail to comply, 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 related to the Codes 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. Ultimately, sanctions and enforcement function primarily as a deterrent against noncompliance and as a means of ensuring responsiveness from member companies, rather than as a demonstration of the NAI's efforts through detailed disclosure of every issue discovered by NAI staff.

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, as noted

earlier. 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.⁴⁷ 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.

Investigations

In 2017 NAI staff conducted six investigations of potential material violations of the Codes. In each case NAI staff found that the member companies in question did not materially violate the Codes, or that incomplete information and misunderstandings caused the investigations, and consequently sanctions procedures were not appropriate.

The first NAI investigation involved the presence of an NAI member company on a website aimed at LGBT audiences. NAI staff investigated to verify whether Opt-In Consent requirements for Sensitive Data were met. In this case, NAI staff determined that the company was functioning only as a technology platform, fully controlled by the publisher of the website, and that the terms of service the publisher presented to all of its registered users disclosed the collection and potential sharing of such data.

The second investigation involved an NAI member appearing to engage in Cross-Device Linking, based on responses to the NAI compliance questionnaire, but failing to meet notice and choice requirements in the NAI's Guidance on Cross-Device Linking. The investigation revealed that the company had not yet launched any Cross-Device Linking products, and was only in the planning and testing stages. NAI staff confirmed that the company met all guidance requirements before launching the product.

The third compliance investigation resulted from a member company's public marketing materials, which appeared to suggest that merger of PII and Non-PII may take place. The investigation revealed that the company did not collect or receive any PII, and that its marketing materials were overzealous in this regard in an attempt to make the technology appear more compelling to clients. The company agreed to be more mindful of the privacy implications resulting from its marketing claims on a going-forward basis.

The fourth compliance investigation resulted from a public enforcement action by another self-regulatory body, alleging a failure by a member company to ensure that notice of its data collection was present on partner sites. NAI staff spoke at length with representatives from the evaluated member company, and determined that the company included contractual requirements for such notice with all partners. However, a portion of the contracts were far more specific in such requirements, while others were vaguer. The company also informed NAI staff that it also makes an effort to manually review partner websites for the presence of the

required disclosures. From an NAI Code perspective, the potential shortcoming in meeting the requirements in question, due to vague language in some of the contracts, did not rise to the level of a material violation considering the company’s countervailing efforts to ensure adequate notice.

The fifth and sixth investigations by NAI staff were initiated by discoveries, during the annual compliance review, that two evaluated member companies may not have been setting all of the opt-out cookies that were necessary to ensure a complete opt out from their IBA activities. NAI staff questioned the companies’ staff and determined that in both cases the opt outs provided by the companies appeared to cover a considerable majority of their IBA activities, and that any missing opt-out cookies would only have limited effect on data collection and use. Both issues were resolved after notification from NAI staff. These were issues that NAI staff expected it could identify as soon as they occurred using its monitoring processes. Failure of the monitoring tools to quickly identify the issues prompted the NAI to make extensive changes to its monitoring software and procedures to improve the tool so as to more rapidly alert members regarding opt-out functionality on the NAI site.

As was the case during prior annual compliance reviews, in 2017 NAI staff found a variety of lesser potential problems with a few 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 became material violations of the Codes. The NAI’s approach helped fix issues expeditiously, while reserving sanctions primarily for instances in which member companies are otherwise unwilling to make requested changes, or fail to cooperate with NAI staff, thus helping to ensure the vitality of the ecosystem.

The NAI’s approach to compliance helped fix issues expeditiously, while reserving sanctions primarily for instances in which member companies are otherwise unwilling to make requested changes, or fail to cooperate with NAI staff, thus helping to ensure the vitality of the ecosystem.

SUMMARY OF FINDINGS

NAI staff found that in 2017 evaluated member companies overwhelmingly complied with the Codes, and to the extent that any potential 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 validates the role of the NAI's Codes and self-regulatory process in promoting consumer privacy in the digital advertising industry. The NAI continues to update its Codes and guidance to keep pace with technological developments and changing norms. Likewise, NAI members continue to devote valuable resources to cooperate in the NAI's thorough annual reviews of their policies and practices. **The common goal is to ensure that members adhere to privacy principles embodied in the NAI Codes and guidance when offering new and existing products, even at a time of global regulatory uncertainty.**

At a time when the nature of digital advertising is being questioned and reconsidered in Europe, it is even more important for self-regulatory efforts in the United States to clearly establish that a thoughtful and flexible self-regulatory approach can provide robust consumer privacy protection while also allowing the digital advertising economy and technology to flourish, and perhaps most importantly, preserving free and equal consumer access to a bounty of diverse content online.

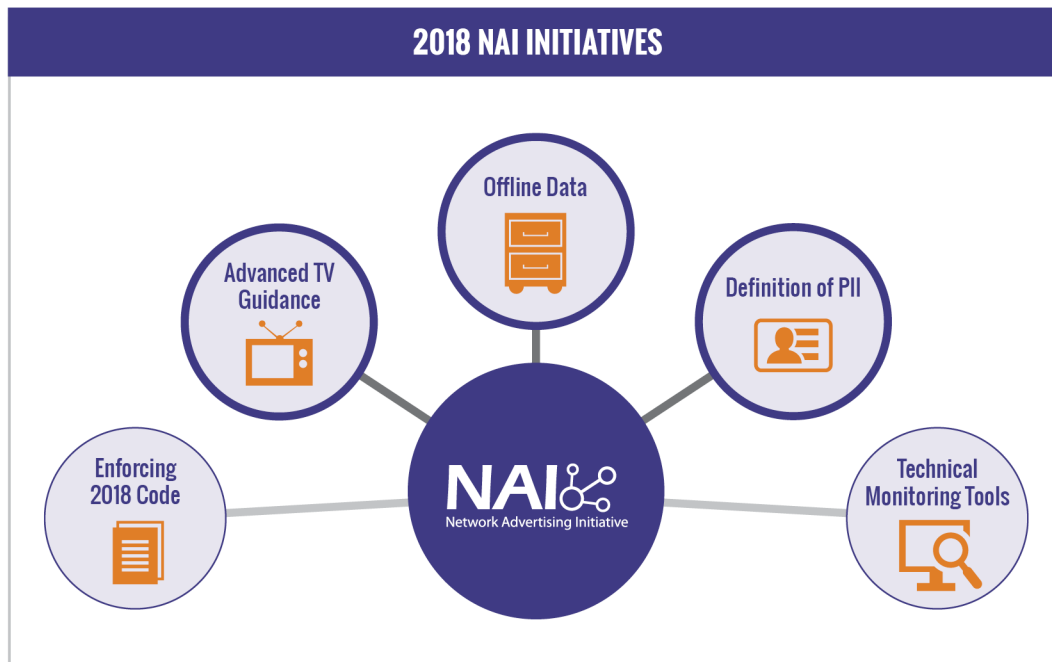
In 2017 the NAI performed its largest compliance review yet, with 96 evaluated member companies, while separately reviewing thirteen additional companies who were accepted as new members during the year. Through this review, NAI staff closely monitored the digital advertising ecosystem, staying current with the latest developments and challenges.

In addition to performing compliance reviews, during this time the NAI also launched a new Code of Conduct, combining previously separate documents into one while simplifying compliance for members and clarifying requirements for consumers. This process allowed the NAI to revisit terminology that had grown somewhat stale over the years. 2017 also marked the publication of Guidance on Cross-Device Linking, and the launch of a completely revamped and reengineered opt-out tool in conjunction with the DAA.

At a time when the nature of digital advertising is being questioned and reconsidered in Europe, it is even more important for self-regulatory efforts in the United States to clearly establish that a thoughtful and flexible self-regulatory approach can provide robust consumer privacy protection while also allowing the digital advertising economy and technology to flourish, and perhaps most importantly, preserving free and equal consumer access to a bounty of diverse content online.

To that end, the NAI is treating its most recent Code update as a springboard for possible significant changes to the Codes in 2018. The NAI plans to evaluate potential coverage of new data sources, such as “offline” data, and to conduct a full review of the nature of “personal” information. As Cross-Device Linking makes it possible for companies to collect data on televisions for advertising use on mobile or desktop devices, or vice versa, the NAI is devoting many resources to drafting guidance on this topic that would ensure that such data collection and use happens in a manner consistent with underlying NAI principles. A new advertising campaign, launched in 2017, is gaining critical mass in 2018. This campaign will help guide users to the NAI’s education content, which is also under revision this year to reflect the newest products and technologies in digital advertising.

The feedback loop of drafting policy to preserve consumer privacy in the digital advertising ecosystem while conducting annual reviews of the companies that compose a large portion of this market, allows the NAI to identify the most pressing and timely issues and challenges, and to address them in a swift and effective manner, which it will continue in 2018.



NAI 2017



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 formally 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,” (ADR) 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 data about a computer or device for the purpose of delivering ads or providing advertising-related services.” ADR includes providing an advertisement based on a type of 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. Unless noted otherwise, all references to the NAI Code and NAI App Code in this document refer to the 2015 Update to the NAI Code of Conduct and the 2015 Update to the NAI Mobile Application Code, respectively.

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. J. HOWARD BEALES & JEFFREY A. EISENACH, AN EMPIRICAL ANALYSIS OF THE VALUE OF INFORMATION SHARING IN THE MARKET FOR ONLINE CONTENT (2014), <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: https://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf.

9 *Guidance for NAI Members: Cross-Device Linking* can be found at https://www.networkadvertising.org/pdfs/NAI_Cross_Device_Guidance.pdf.

10 2018 NAI Code of Conduct can be found at: https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf. The Code also includes commentary that is intended to illuminate the intent behind certain provisions; commentary is not intended add any substantive obligations to members or change the principles of the Code.

11 *Informational Injury Workshop*, FEDERAL TRADE COMMISSION, <https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop>.

12 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.; see also App Code § I.K).

13 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.

14 The following thirteen companies completed the new member application process and became NAI members in 2017: BounceX, Clickagy, Freckle IoT, Fysical, Ibotta, inMarket Media, Media iQ, Netmining, Outbrain, Reveal Mobile, SambaTV, Taboola, Throtle.

- 15 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 recommendations to comply with the Codes' 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.
- 16 See Investigations and Sanctions *infra* pp. 31-33.
- 17 The following companies were reviewed in 2016 but were not among evaluated member companies in 2017:
- a. Circulate, LinkedIn, Madison Logic, TellApart, and X+1, were no longer independently engaged in IBA and CAA operations in the United States. These companies terminated their NAI memberships and did not complete the 2017 annual compliance review.
 - b. ChoiceStream and Audience Science ceased operations altogether in 2017.
 - c. MaxPoint, Dstillery, and Optimatic did not renew their NAI memberships in 2017.
- 18 See *supra*, note 14.
- 19 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.
- 20 If a member has an agreement with a partner to collect data on the partner's site or app 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.). See Pass-On Notice *infra* p. 21.
- 21 NAI member companies comprise all of the top 10 Ad Networks according to the comScore Ad Focus Rankings (Desktop Only), available at <https://www.comscore.com/Insights/Rankings> (last visited March 26, 2018).
- 22 See <https://www.internetaalerts.org/>.
- 23 See <https://www.cuebiq.com/data-for-good/>.
- 24 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 secrets. However, members are expected to provide general descriptions of the technologies they are using for IBA, CAA, and/or ADR.
- 25 As described above, with the Privacy Disclosure Scanner, the NAI monitors member privacy disclosures to ensure that members do not inadvertently remove language required by the Codes.
- 26 See Enhanced Notice Requirement *infra* p. 21.
- 27 The NAI determined that some evaluated member companies did not collect data, but instead facilitated others' collection of data for IBA or CAA purposes, such as advertising technology platforms. The NAI encourages, but does not require, these members to ensure that proper notice is provided where their technology is used to collect data for IBA or CAA purposes. The NAI found during the compliance review that many such evaluated member companies nonetheless provided such notices.
- 28 The NAI's compliance reviews are limited to the practices and disclosures of its members.
- 29 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. In concert with the DAA, the NAI expects to issue a formal compliance notice, before enforcement of this requirement is implemented sometime in 2018.
- 30 Opt-In Consent means that "an individual takes some affirmative action that manifests the intent to opt in" (Code § I.I.; App Code § I.J.).
- 31 Many evaluated member companies did not employ "standard" interest segments at all, but rather engaged only in practices such as Retargeting, or custom segmentation.

- 32 Although this terminology has been revised for 2018, and is now referred to as Device-Identifiable Information, in 2017 the NAI defined Non-PII as “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.; see also App Code § I.E).
- 33 See, e.g., *Opt Out of Interest-based Ads in the App Store and Apple News*, APPLE, <https://support.apple.com/en-us/HT202074> (last visited Feb. 25, 2018).
- 34 See <http://youradchoices.com/appchoices>.
- 35 See <https://www.networkadvertising.org/mobile-choice>.
- 36 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.
- 37 See <http://www.networkadvertising.org/faq/#n178>.
- 38 See the Introduction and Commentary to Code.
- 39 See http://www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf.
- 40 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.).
- 41 See http://www.networkadvertising.org/sites/default/files/NAI_ImpreciseLocation.pdf.
- 42 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.).
- 43 See NAI Code, *supra* note 7 at 15.
- 44 Independently of NAI Code requirements, member companies are, of course, expected to abide by the laws applicable to their businesses.
- 45 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 or CAA, 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.
- 46 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.
- 47 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