Network Advertising Initiative: 100+ AdTech Companies Self-Regulate Digital Advertising Standards for Responsible Consumer Data Collection

BLOG POST

By: Sean Garrity
Posted: July 25, 2017

Follow "The Hosting Blog" daily as hosting experts, programmers, and tech managers go in depth on a variety of tech-related topics.

👍 Like 1   🐦 Tweet   G+

TL; DR: *For nearly two decades, AdTech companies have been working together as part of the nonprofit, self-regulatory association Network Advertising Initiative (NAI) to develop approaches to online advertising that promote responsible data collection and use practices. The organization aims to build pragmatic strategies and standards that benefit all stakeholders — the publisher, the advertiser, and, most importantly, the consumer. By implementing flexible self-regulation and a strict policy of compliance and enforcement, NAI helps businesses use targeted advertising without infringing on users' privacy rights. This results in peace of mind for consumers and ensures the ads presented to them in the digital space are relevant and create more personalized online experiences.*

In 1999, the Electronic Privacy Information Center (EPIC) raised concerns over the proposed acquisition of Abacus Direct, the US's largest catalog database firm at the time, by DoubleClick, the web's biggest advertising company. Because Abacus's vast database contained more than 88 million buyer profiles built with data from upward of 2 billion purchase transactions, EPIC worried that consumer privacy would be compromised when browsing and shopping online.

The top network advertisers of the day were quick to take notice of these growing privacy fears and decided to band together do something about it. This led to the creation of the nonprofit, self-regulatory association Network Advertising Initiative (NAI) and the first program to set forth rules on how and when advertisers can combine web browsing data with personally identifying information (PII).

NAI's Anthony Matyjaszewski told us how the self-regulatory organization is helping protect consumer privacy online.

"People realized that if you take a company that has all our personal information and merge it with a company that houses web browsing data you can know what kind of websites people are visiting

and tie that to their real names," said Anthony Matyjaszewski, NAI's VP of Compliance and Membership. "NAI was created to address that."

Nearly 20 years later, the more than 100 AdTech companies that make up NAI continue to work together to build and maintain practical standards in online advertising and data collection that benefit all parties of the dynamic — web publishers, advertisers, and consumers. In addition to giving web users peace of mind knowing their information is safe, NAI's policies allow its member companies to deliver more trustworthy and relevant ads to their target audiences, which works to personalize consumer journeys online.

Interest-Based, Cross-App Ads Bring Relevant Content to Consumers

Digital advertising takes many forms and is transmitted mainly through websites and apps. Interest-based and cross-app advertising works by assigning assigning interest categories to cookies and advertising identifiers based on prior browsing activity.

NAI member companies use broad interest groups to appeal to a larger audience, rather than smaller niche audiences. In doing so, these advertisers show ads that are relevant to more people without the need to gather a wealth of potentially invasive data about individuals.

"Most third-party advertising companies are not interested in PII," Anthony said. "And the regulations we've set forth incentivize them to target ads based on non-PII."

Interest-based advertising delivers content based on browsing habits, and NAI ensures advertisers do this responsibly.

But, even without PII, the nature of these interest-based ads are still personalized and targeted and greatly increase revenue for advertisers and publishers. While companies benefit from gathering behavioral data, NAI advocates for a strict balance between the use of this data and how it impacts consumers.

NAI requires member companies to use methods, like cookie and opt-in notices, to let users know that data might be used to personalize their browsing experience, including showing relevant ads and making checkouts quicker.

The organization has enforcement policies in place that keep companies compliant. For example, if the NAI finds a company isn't properly notifying users about its data collection and use practices, it will work with the company to fix the issue ASAP.

Adapting Alongside Evolving Technologies That Gather Consumer Data

Anthony told us that, for web-based data collection, the traditional way to recognize a user from one visit to the next was the use of cookies. These are small text-based files containing basic user info and have a randomized ID that corresponds with a return visitor.

Cookies containing random identifiers can enable companies to keep track of which links a given browser has clicked, or which sites it has visited, and do not typically contain any identifiable information like names and addresses. Though blocking all cookies can make browsing challenging, some browser makers began blocking third-party cookies by default.

"In blocking cookies by default, it is no longer the consumer's choice" Anthony said, "but rather the browser manufacturer's choice."

NAI members gather at the organization's Summit each year to discuss evolving technologies and privacy concerns.

Blocking cookies made advertising as well as analytics difficult for companies, even hindering things like basic user counts and consistent logins. Not only are cookies beneficial to businesses, but they also eliminate the need to constantly re-authenticate accounts across visits.

"As cookies were being blocked, companies had to improvise by using data points, such as IP addresses and U/A strings, to recognize browsers across sessions," Anthony said. "We told our members that if they use these technologies, they would have to provide transparency."

This way, NAI makes it possible for members to still engage in targeted advertising and maintain the consumer trust that their information is not being used without permission.

The Key Value of Membership: Peace of Mind for All Stakeholders

According to Anthony, every member of NAI must be vetted through an exhaustive review process. The organization looks at every item that relates to complying with its privacy policies, including contract language, disclosure statements, and data flows.

NAI also re-evaluates its members on an annual basis to account for business model changes and emergent data technologies.

"Many data policies are just clipped from another website, especially when it comes to smaller publishers," Anthony said. "It tends to be very cut-and-paste, but a lot of these were drafted in that cookie-based world."

These privacy policies notify users that they can opt out of cookies or block them with browsers. However, since more publishers are working with companies that may use non-cookie technology, those notices could be outdated. NAI thus ask its members to push publishers to update their disclosures.

Brand trust is important, and NAI members are seen as compliant and trustworthy by consumers, thus building rapport that benefits everyone — consumers, publishers, and advertisers.

"Knowing that NAI members go through a stringent review process from our team helps give peace of mind to partners," Anthony said. "Advertisers, publishers, other AdTech companies, and consumers all know that they are working with a reputable company."

Targeted advertising is used with respect to visitor interests — if a user wants a personalized ad experience, they can have it — and companies will benefit as a result.

An Ongoing Effort to Meet the Challenges of Multi-Device Advertising

Just as the merger of the large database and advertising firms raised concerns in the late 1990s, multi-device advertising, while effective, raises unique challenges for privacy protection today.

"They could be showing an ad on one device based on data from another device," Anthony said. "There's more room for privacy infringement."

Many mobile apps, especially free versions of paid apps, display ads and even collect user data for further advertising purposes. These ads help monetize mobile platforms for publishers but are still required to disclose their methods of data collection and what the gathered data may be used for. As new advertising technology and platforms emerge, NAI has updated its guidelines accordingly to keep end users in the loop regarding the use of their data.

"Our most recent guidance is our cross-device guidance," Anthony said. "From an analytics perspective, if both a laptop and a phone are coming from the same IP address, you can see traffic from the same user."

Because mobile browsing habits have more outside influences, they often differ from at-home browsing habits. By analyzing both sources of traffic, advertisers can get a better picture of a user's interests and concerns. Cross-platform advertising also helps publishers monetize their content with broader exposure.

NAI's efforts to solve the privacy issues associated with today's multi-device advertising techniques spotlight the association's continued commitment to developing strict regulatory advertising standards that not only protect consumers but ensure the credibility and brand trust of advertisers and publishers.