100

BBB Online Interest-Based
Advertising Accountability Program

100 PUBLIC ACTIONS

A RETROSPECTIVE

BBB

BBB Online Interest-Based Advertising Accountability Program

100 PUBLIC ACTIONS

A RETROSPECTIVE

Executive Summary

The Online Interest-Based Advertising (Accountability Program) launched in 2011 as an independent enforcer of the Digital Advertising Alliance's (DAA) then-new self-regulatory privacy principles. Over the program's eight-year existence, it has released 100 public actions applying the DAA's Principles.* This report explores the major themes and accomplishments of the Accountability Program's enforcement work.

As described in this report, the creation of a comprehensive set of privacy principles for digital advertising was a major step by the industry. However, in creating this new framework, the digital advertising industry went further and created an independent accountability process which would monitor covered companies for compliance with these standards, publicly report its findings, and refer cases of uncorrected non-compliance to the appropriate regulatory agencies. To provide these "teeth" to the program, the DAA turned to the Council of Better Business Bureaus—which for almost 50 years has administered a suite of programs providing self-regulatory oversight for advertising industry practices.

The Accountability Program's enforcement, as is true of other self-regulatory programs administered by the Council of Better Business Bureaus, is conducted in a transparent and impartial manner. To date, nearly all industry members subject to review have voluntarily complied with the program findings, demonstrating that industry views the DAA Principles as important and the Accountability Program as objective and fair. In the rare event where companies choose not to follow through with the self-regulatory process, the program has referred cases to the appropriate government authorities.

The Accountability Program has spent ample time in both the traditional desktop computing and mobile computing spaces, with 66 cases involving desktop-related issues and 13 involving mobile issues. The Accountability Program's work has touched on a variety of points, but its consistent focus has been on several key items: ensuring consumers are provided enhanced notice, making sure that third parties' opt-out tools exist and are functional,

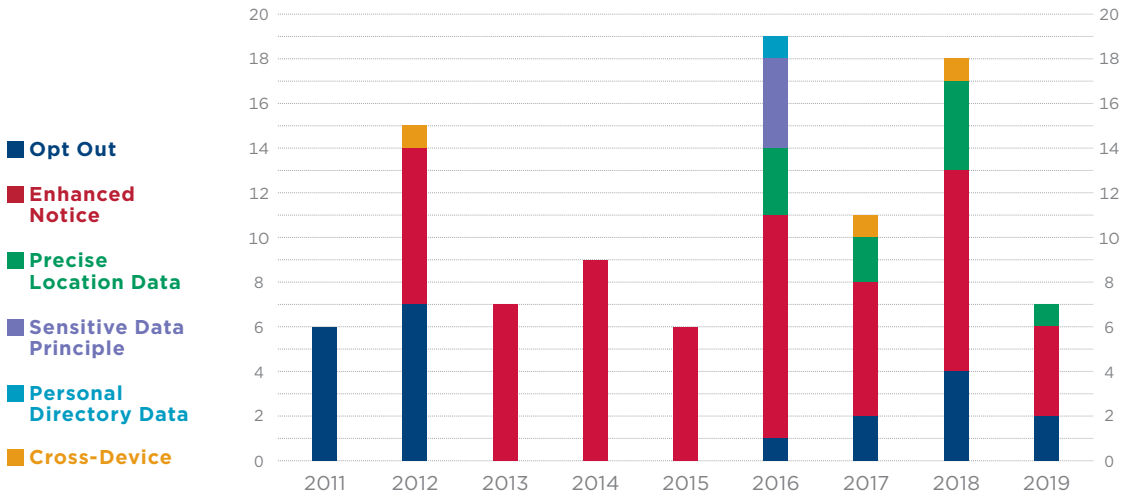
* The majority of these actions have been "cases," or formal published reviews of companies' privacy practices, which have illuminated nearly every corner of the DAA's ever-evolving digital privacy standards.

adapting to the burgeoning mobile app marketplace, and grappling with emerging technologies like cross-device targeting. A sampling of these issues can be seen in Figure 1, below.

84%
of cases focused on **enhanced transparency**

FIGURE 1

Number of Issues Covered in Decisions and Dispositions by Issue Type from 2011 to 2019 YTD



Of the cases released to date, fully 58 have brought home the importance of providing timely "enhanced" notice to consumers—one of the novel components of the DAA Principles that has raised the bar for privacy information disclosures. The Accountability Program has also worked to protect children's privacy in three cases that reflected on

38%
of cases focused on **providing consumers with choice about interest-based ads**

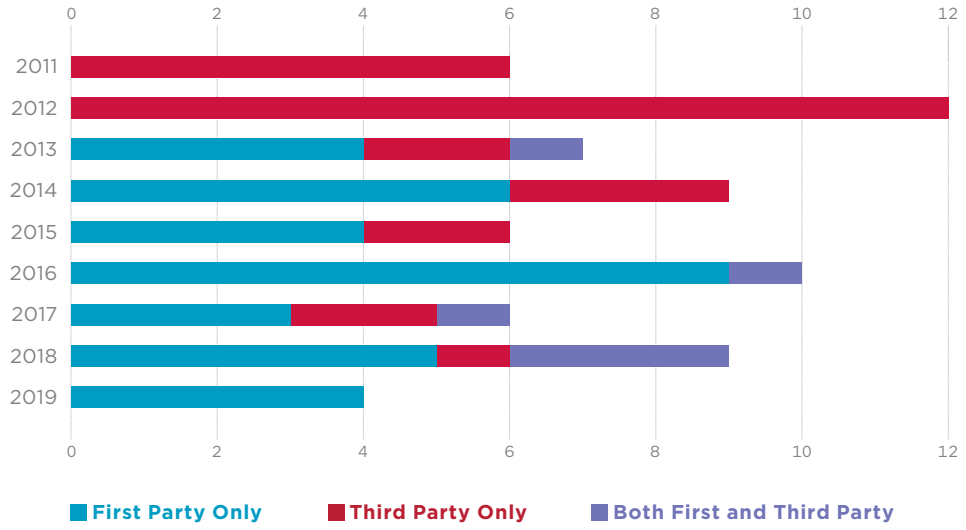
19%
of cases involved **mobile device enforcement**

the intersection of the Children's Online Privacy Protection Act and the DAA Principles, and it has tackled the sensitive topic of companies gathering users' precise location data through mobile apps in 10 of its reviews. Importantly, drawing from its more than 17,500 consumer complaints over the years, the Accountability Program has initiated 13 cases based on tips from the public.

The Accountability Program has also been even-handed in its approach to web publishers—so-called "first parties" under the DAA Principles—and advertising technology companies, or "third parties." It has issued 35 cases involving only first parties, 28 involving only third parties, and six in which the party sat in both positions.

FIGURE 2

Number of Decisions and Dispositions Applying First-Party Provisions, Third-Party Provisions, or Both from 2011 to 2019 YTD



This body of work—which includes detailed technical analyses of websites, mobile applications, and advertising technology—has guided industry, privacy advocates, legislators, marketing professionals, and attorneys in navigating the online advertising privacy landscape. Today's report memorializes the 100th public action of the self-regulatory unit by exploring the history of the Accountability Program and highlighting some of its most important casework.

Prologue

In the few short decades since William Gibson coined the term "cyberspace," the concept of a global super-network through which people can communicate and conduct business with near-instantaneous speed has leapt from the pages of speculative fiction into reality with irresistible force. The rise of the global commercial internet has fundamentally reshaped markets and cultures alike, with knock-on effects on everything from politics to urban development. In this unfolding story, a core chapter focuses on the relationship between consumers and businesses that is established through the practice of data-driven "interest-based" advertising, also known as tailored or targeted advertising. As the internet has altered the world that gave birth to it, advertising has shaped the digital media that now overwhelmingly carry it, and in so doing, has positioned itself at the nexus of critical marketplace and cultural issues: consumer privacy in the digital world.

Interest-based advertising, or "IBA," is the practice of using data about consumers' online activity to infer their likely interests and reach them with ads that are calculated to match those interests. Whether serving automobile ads to an individual who has recently begun researching the latest model-year releases or enticing an avid shopper with an item they had been looking at earlier in the day, IBA aims to be relevant to the individuals who see it. In the ideal scenario, an interest-based ad serves all sides of the transaction: consumers get less annoying, more appealing ads; advertisers can more reliably reach their target audience, allowing greater return on their ad investment; and publishers receive higher payments for running valuable interest-based ads, with their relatively high rates of customer engagement.

In the ideal scenario, an interest-based ad serves all sides of the transaction...

Yet, even as consumers reaped the benefit of this type of advertising, concerns about data privacy grew. Netizens experienced trepidation about ads that seemed to follow them across disparate websites in a manner that seemed to note their comings and goings around the web. Consumer concern made its way to advocacy and regulatory bodies, culminating in a pivotal Federal Trade Commission (FTC) report recommending a set of best practices for conducting IBA in a way that honors consumers' privacy.

In recognition of consumers' concerns, and drawing on the FTC's recommendations, the online ad industry formed an advertising privacy consortium called the Digital Advertising Alliance to develop baseline privacy standards for IBA. Working with expert advisors from the online ad industry and beyond—including the Council of Better Business Bureaus—the DAA drafted and promulgated the **Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles) in 2009**.

The OBA Principles set out industry best practices for the collection and use of data for IBA in the form of seven principles. In short, these principles called for ad tech companies to provide disclosures of their practices and opt-out tools, and they entreated advertising providers and website publishers alike to provide users with just-in-time "enhanced" notice. Critically, the DAA also developed an in-ad signal—the now-familiar AdChoices Icon—that afforded consumers a recognizable, uniform symbol to click in order to learn about IBA and, should they choose, opt out.

Crucially, the substantive principles were fortified by the Principle of Accountability. By implementing an independent accountability mechanism, the DAA did more than promise self-regulation. It delivered on this promise and, in the process, derived legitimacy from independent enforcement by an organization with a reputation for building trust between consumers and businesses. The Council of Better Business Bureaus was given this role, culminating in the creation of the Online Interest-Based Advertising Accountability Program in 2011.

The DAA Principles and the Accountability Program serve as two pillars of a self-regulatory structure that promotes responsible commercial activity and protects consumer privacy. Through its enforcement work, as this document shows, the Accountability Program has demonstrated the effectiveness of well-designed self-regulation.

What Have We Learned?

Figure 1 laid out the issues the Accountability Program has tackled over its eight years of operation (page 2). This simple chart tells a number of stories, ones about changes in the market, the growth of the DAA Principles, and the commensurate evolution of the Accountability Program's enforcement initiatives.

Enhanced Notice

Throughout its history, the Accountability Program has placed a major emphasis on ensuring that companies provide enhanced notice about IBA. This is not by accident. While the Accountability Program's earliest cases covered a number of simple ad tech issues, the Accountability Program quickly noticed that enhanced notice—particularly the kind supplied by website publishers—needed serious attention before it could meet the promise of the Principles. Digital advertising companies, located at the heart of the online advertising ecosystem and thus more familiar with the rules of the road, had quickly worked out many of the technical kinks that impeded compliance in the earliest days of the DAA Principles. But many website publishers mistakenly believed that only these ad tech firms had compliance responsibilities under the DAA Principles, a misconception that the Accountability Program tackled head-on by releasing its first **Compliance Warning**. This document explained in detail the responsibilities of website publishers, particularly about providing enhanced notice on their websites, and it set a firm deadline of January 1, 2014, after which vigorous enforcement of this point would begin.

> ...one of the most difficult aspects of IBA... is its relative imperceptibility to the average user.

This issue matters because one of the most difficult aspects of IBA from a privacy perspective is its relative imperceptibility to the average user. The DAA Principles attempt to tackle this natural feature of the practice by intentionally surfacing the collection and use of data for IBA in the form of a timely, in-your-face notice. Industry coalesced early around a single icon, the AdChoices Icon, creating a de facto unified symbol for representing the fact that data was being collected for IBA on a specific website or used to serve a specific ad.

As **Figure 1** indicates, the Accountability Program has worked consistently to apply these rules, starting with its Facebook case in 2013, moving through its first compliance warning, and maintaining this focus as its work expanded into the mobile world. Even as other issues emerged—children's mobile apps collecting precise location data or native ads being targeted based on prior browsing behavior—enhanced notice enforcement has remained a significant substratum of the Accountability Program's casework.

According to Accountability Program complaint data, consumers are increasingly aware that website operators allow IBA on their sites, and they have become more vocal when these companies do not provide adequate notice and access to user controls. As a result of these consumer complaints, the Accountability Program brought a number of actions involving well-known brands with major web presences, including Panasonic, Budweiser, Finish Line, the Northern California branch of the American Automobile Association, and Publishers Clearing House.

Critically, the Accountability Program also reminded third parties that, as owners and operators of websites that allow non-affiliate IBA, they also bore first-party responsibilities. In the Varick Media Management case, where third parties appeared to be collecting data for IBA on the Varick website, the Accountability Program had the company add an enhanced notice link to its website footer to ensure that visitors were aware of this background collection. This case illustrated to industry that third-party ad tech companies, when authorizing data collection on their own websites, must follow the requirement for website publishers to provide enhanced notice to their users.

Finally, a combination of consumer complaints and in-house monitoring resulted in more work on the enhanced notice front over 2018 and 2019, including actions focused on direct-to-consumer brands like Purple, Ledbury, and Mizzen and Main. These budding direct-to-consumer sales companies are a booming part of the online economy that routinely use IBA as part of their overall marketing strategy. The Accountability Program's actions here were an attempt to raise awareness in this subset of the online marketplace.

Through years of compliance actions, the Accountability Program has worked to ensure that consumers have access to clear disclosures about IBA

and links to opt-out tools when they visit their favorite sites. These cases also demonstrated that web publishers are responsive to consumer concerns and acknowledge the role the Accountability Program plays as a neutral, independent adjudicator of both commercial and consumer interests.

The Mobile Transition

In the early 2010s, the world witnessed the rapid expansion of smartphone use among the general population, taking the item from an executive status symbol to a fully integrated component of average individuals' lives. Now, many users have begun using their mobile device as their primary gateway to the internet. Consequently, the technological landscape has shifted dramatically over the past decade; the earlier world of an internet accessed by web browsers has morphed into the world of mobile apps, which are specialized programs tailored for mobile operating systems. Just as advertisers and tech companies had joined with website publishers to reach consumers through the earlier channels of the internet, these entities fashioned their technologies to reach consumers in mobile apps and deliver IBA in this evolving new format.

...the world witnessed the rapid expansion of smartphone use among the general population...

Forecasting the privacy concerns that would arise in this new frontier, in 2013 the DAA issued the Application of the Self-Regulatory Principles to the Mobile Environment, also known as the **Mobile Guidance**. This document translated the original best practices of the OBA Principles into the mobile world, carving out requirements for notice, enhanced notice, and opt-out mechanisms for app publishers and third-party ad tech companies. The Mobile Guidance established best practices for engaging with new types of data, such as "cross-app data," which include device identifiers, and precise location data (the data derived from a number of different technologies, including GPS satellites and WiFi networks, that can determine the location of a user or their device).

The release of the Mobile Guidance served as a testament to the agility of self-regulation, as the document represented a swift translation of industry best practices for privacy in the desktop realm to the expanding universe of mobile apps. As the issues chart in **Figure 1** makes clear, enforcement began quickly, with the publication in 2016 of the first

mobile case decisions dealing with such issues as precise location data and children's privacy.

Major Mobile Themes

Starting in October 2015, the Accountability Program applied its technical expertise to the world of mobile apps, reviewing numerous applications in the Google Play Store and Apple App Store online marketplaces. Using a variety of modern digital forensics methods, the Accountability Program combed through network traffic and reviewed the privacy policy documentation of app publishers. This culminated the following year in the release of its first mobile compliance actions.

The Accountability Program's first mobile releases focused on gaming apps with massive user bases and apps that authorized the collection of precise location data. The compliance roundup was a success, as app publishers worked cooperatively to revise their privacy disclosures, add enhanced notice, and where necessary, disable the collection of certain types of data. In 2016, the Accountability Program's mobile app reviews included major brands, like top mobile game publisher SEGA and the medical insurance company Aetna.

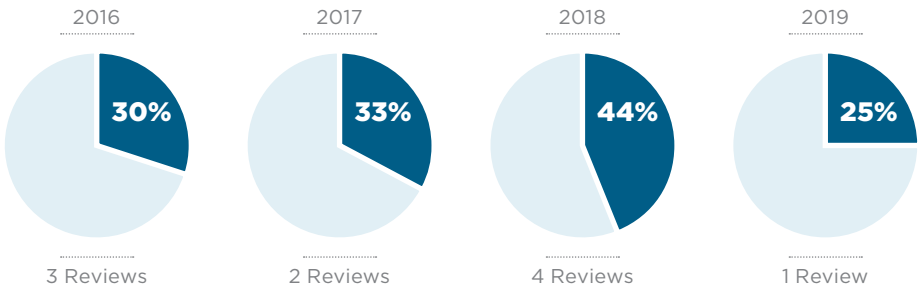
The Accountability Program has also tackled many cases involving the special data categories described by the Mobile Guidance. Of those, one of the most important and frequently encountered is precise location data, which refers to data precise enough "to locate a specific individual or device." The drafters of the Mobile Guidance were cognizant of the sensitivities surrounding this category of data, which has the potential to reveal the most intimate details of a person's life. Precise location data, after all, can track an individual through time and space as they move between locations, such as from their home to a political rally or a doctor's office. Consequently, the Mobile Guidance requires companies to obtain consumers' consent when first parties authorize the collection of precise location data for IBA purposes.

The first case in this vein was Spinrilla, the maker of a hip-hop mix-tape app, and a recent one involved major shoe retailer Finish Line. These cases exemplify the two main approaches to aligning with precise location data best practices taken by app developers. In the case of Spinrilla, the Accountability Program's decision outlines that the company did not have

sufficient use for this precise location information, so it opted to disable the collection of precise location data through its app. This obviated the need to add location disclosure information to its app or to obtain consumers' consent to let third parties use this data for IBA. Contrariwise, the Accountability Program's decision in the Finish Line case explained that the company wished to continue using this sort of data. Consequently, Finish Line worked with the Accountability Program to build a custom enhanced notice and consent tool that informed consumers about the third-party collection of precise location data through its app. The company also engaged in a comprehensive update of its privacy policy documentation, including adding new location disclosures. Though starkly different, both companies' solutions fit the terms of the DAA Principles.

FIGURE 3

Percentage of Decisions and Dispositions Involving Precise Location Data from 2016 to 2019 YTD



The Accountability Program's mobile app case releases have also been significant in their examination of mobile apps apparently directed at children. As the Mobile Guidance translates all provisions of the OBA Principles to the mobile space, it brings along the Sensitive Data Principle, which includes provisions incorporating the Children's Online Privacy Protection Act of 1998. The Accountability Program applied this Principle during its initial mobile app cases, working with the app developers Top Free Games, Bearbit Studios, and SEGA to ensure that their products followed industry standards with respect to the digital privacy of children. As the years went on, the Accountability Program and its sister program, the Children's Advertising Review Unit, teamed up to tackle children's privacy in mobile apps. In March of 2019, the programs referred the game

publisher HyperBeard to the FTC for failing to respond to their joint inquiry about the company's data privacy practices—particularly regarding the possible collection of children's data. This event demonstrated that effective self-regulation, while voluntary, is backstopped by the possibility of referral to the appropriate government authority.

Third Parties and Opt-Out Tools

The Accountability Program has paid close attention to the opt-out tools provided by ad tech companies since its earliest days. The first cases on this point largely concerned improper deployment of an opt out. For example, in QuinStreet, the Accountability Program found that the company's opt-out link was visible to varying degrees depending on which browser was used to render it. According to the decision, this would have made opting out impossible for users of Mozilla's Firefox browser and difficult for users of other browsers. And in Martini Media, it appeared to the Accountability Program that the company's opt-out tool set a cookie that lived for too short a time, rendering the opt out less effective than the industry standard. Ensuring that opt-out tools were properly configured and deployed was essential during the formative years of the DAA's AdChoices program.

As one might expect, companies quickly incorporated the basics of opting out into their technology and compliance strategies. Of course, all implementations require maintenance, and the Accountability Program kept an eye out to see that the machinery underlying companies' opt-out mechanisms functioned correctly. In its 2016 case involving the agency trading desk Varick, the Accountability Program found that Varick's in-ad enhanced notice links failed to function. Furthermore, between broken links and unreasonably long load times, the Accountability Program noted that the company's privacy policy and opt out were inaccessible even on its own website. In the end, Varick undertook significant work to catch up on its deferred maintenance.

The technical differences between desktop and mobile computing opened up new opt-out implementation issues in the latter half of the 2010s. One fundamental issue dominated this area: the usability of mobile opt-out mechanisms. Though the DAA had published

The technical differences between desktop and mobile computing opened up new opt-out implementation issues...

its “AppChoices” app in 2015, companies were free to implement their own mobile opt outs just as they had done on the web. But this task proved more complex, as shown in the 2017 Adbrain case. According to the decision, the company provided consumers with a text-entry form that required users to manually type in their “device ID.” However, the Accountability Program found that the company did not provide sufficient instructions for users to understand how to complete the form, rendering the opt out too difficult to use. A similar case from 2018, Kiip, involved another text-entry opt-out form that the Accountability Program believed lacked sufficient instructions to make it easy for an average user to complete. In both cases, the companies made modifications to their opt-out tools to render them easy to use.

Cross-Device Evolution

Self-regulation’s ability to evolve alongside technology is again on display in the history of cross-device advertising. Cross-device advertising is a marketing practice that bridges the worlds of desktop and mobile devices. In the earlier days of the internet, a user might have only accessed the web through one or two devices. As the internet evolved, the number of devices in a household multiplied; many users possessed not only a home desktop computer and a smartphone, but a laptop, a tablet, and a work computer. Advertisers and ad tech companies followed consumers across their multi-device journey, and cross-device advertising was born. Now, companies routinely associate data across multiple devices to build a data profile on a particular consumer or household for the purpose of delivering IBA.

The Accountability Program first addressed this issue in its 2012 BlueCava case, which examined this data management platform’s nascent cross-device practices. The Accountability Program found that while the company created “households” by associating devices linked to the same residence, its disclosures were silent on the subject. The decision also explains that BlueCava maintained two IBA opt outs, but that its disclosures were unclear regarding the scope of the opt outs—would they be applied to one device or a whole household of devices? The Accountability Program was also concerned about the difference, if any, between the two tools. As a result of this review, BlueCava amended its disclosures to indicate that it may collect data across a user’s set of devices for IBA and pledged to pioneer a multi-device opt out.

BlueCava represented an early look at an emerging practice. The DAA recognized that adoption of this practice would no doubt accelerate, and industry would look to the DAA Principles for best practices about how to honor consumer privacy while creating device graphs to reach their preferred audiences. Anticipating the need for guidance about how to apply the existing DAA Principles to this practice, the DAA issued the **Cross-Device Guidance in 2015**. And after a two-year period for companies to adapt to the guidance, the Accountability Program announced in 2017 through a **Compliance Warning** that it would commence enforcement.

At the end of 2017, the Accountability Program lived up to its promises to consumers and industry, issuing its first ever cross-device case: LKQD Technologies, Inc. The Accountability Program found that LKQD had been collecting data for IBA through a popular women's health app, including precise location data and cross-app data. The Accountability Program also found that part of the company's business practices involved associating different devices with a single user or household. As a result of the Accountability Program's review, LKQD updated its privacy notices to describe that it engaged in cross-device tracking and to provide consumers with the ability to opt out of this type of advertising on each of their devices. Through this case, the Accountability Program again demonstrated the capacity of the DAA Principles to flow alongside new technologies and use cases, providing consumers with choices about their privacy no matter what platform or technology they use to reach the internet.

...providing consumers with choices about their privacy no matter what platform or technology they use to reach the internet.

2018 also saw another instance of cross-device enforcement, as the Accountability Program discovered the company Kiip collecting data for IBA through a popular exercise app. After noting possible compliance deficiencies, the Accountability Program worked with Kiip to bring the company up to spec with the Cross-Device Guidance. As explained in the decision, Kiip upgraded its privacy policy, making the device-specific extent of its opt-out tools clear to consumers.

Conclusion

So what do all of these lessons add up to? All of these cases—all of these patterns of enforcement—show several simple, concrete processes and principles at work:

Be Efficient

The Accountability Program, like any enforcement entity, must make intelligent decisions about how to most effectively commit its limited resources. On any given Thursday, do you focus on static analyses of children's apps? Web crawls of the Alexa Top 1000? Or do you see a trend that merits a compliance warning—and fast? Through its work, the Accountability Program has tried to answer these questions and others with an eye toward having the biggest effect it can on the most important players and issues in the IBA world. From bringing cases against major companies like Facebook to effecting substantive changes in apps with millions of daily active users, the Accountability Program's work has brought significant parts of the market into step with the DAA Principles.

Be Nimble

The Accountability Program has had to adapt to changing technical practices, legal rules, and industry best practices in order to do its job effectively. From amendments to the Children's Online Privacy Protection Act Rule in 2013—which affected the analysis of children's data collection under the DAA's Sensitive Data Principle—to the transition from desktop to mobile forensic analysis, change has been one of the few constants in the program's work. The Accountability Program has tackled cross-device tracking, interest-based video ads, and non-cookie identification techniques alongside its enforcement staples, often through the vehicle of compliance warnings, which themselves were an adaptation developed to raise awareness and correct market misunderstandings around specific topics. In short, self-regulation must learn from yesterday and anticipate tomorrow.

Be Reasonable

This point may sound unremarkable, but it is probably the most important one. The Accountability Program's position as a neutral enforcement body requires it to check its assumptions and not develop biases, whether for or against any segment of the market. This positioning requires its enforcers to approach compliance analyses and possible remedies from a holistic perspective, with both consumers and businesses in mind. For example, the major focus on enhanced transparency comes from the understanding that it is the gateway to all of the other information and tools required by the Principles. Without enhanced notice links, even the best disclosures and the slickest opt-out tools are likely to go unnoticed by consumers, depriving them of virtually all of the benefits of the DAA Principles. However, businesses have their own, entirely legitimate concerns about reaching compliance, so the Accountability Program has been flexible, allowing for creative compliance implementations, honoring code freezes even where they slightly delay remediation, and understanding all that can go wrong with mobile app redevelopment and rollout. The Accountability Program has responded strongly to the well-formed complaints of individual members of the public—strangers to us, but integral players in our self-regulatory work. And the program always takes into account the size, sophistication, and capabilities of a company under review, recognizing that a Fortune 500 company and a two-man development team are wildly different creatures. Being able to see all sides of an issue, checking assumptions, interpreting the rules in ways that will not surprise or injure the parties involved, all of these keep the Accountability Program true to its mission as part of the larger Better Business Bureau family: to make the market better not for businesses, not for consumers, but for everyone.

Authors

Jon Brescia is the Director of Adjudications and Technology for the Online Interest-Based Advertising Accountability Program at the Council of Better Business Bureaus. Part attorney, part tech guy, he is equally comfortable drafting legal arguments or analyzing network traffic logs. Jon supervises the monitoring and investigation of companies' interest-based advertising practices to ensure that they comply with the Digital Advertising Alliance's cross-industry principles.

Ayaz Minhas serves as Data Privacy Specialist for the Online Interest-Based Advertising Accountability Program of the Council of Better Business Bureaus. In this role, he monitors companies engaged in interest-based advertising in the mobile and desktop ecosystems for compliance with the Digital Advertising Alliance's cross-industry principles for online privacy. A skilled attorney, Mr. Minhas is adept at analyzing technical and policy issues related to data collection for interest-based advertising.

BBB Online Interest-Based Advertising Accountability Program

3033 Wilson Boulevard, Suite 600
Arlington, VA 22201

BBBprograms.org/IBA