

Online Interest-Based Advertising Accountability Program

COMPLIANCE WARNING

SUBJECT: The Digital Advertising Alliance’s Cross-Industry Self-Regulatory Principles are Enforceable Irrespective of the Identification Technology Used.

I. Summary

The Online Interest-Based Advertising Accountability Program (Accountability Program) is one of the two accountability agents¹ charged by the Digital Advertising Alliance (DAA) with enforcing the cross-industry Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles), the Multi-Site Data Principles (MSD Principles) and the Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance) (collectively, the Principles).²

The Accountability Program monitors the actions of all companies in the advertising ecosystem for compliance with the Principles and initiates formal inquiries when it has reason to believe that a company may have a compliance issue. The review process is confidential. However, the Accountability Program issues a public decision or administrative disposition explaining its findings to ensure the transparency of its compliance work and to help educate industry and the general public about the requirements of the Principles. In order to further its education and accountability work, the Accountability Program may exercise its discretion to issue a public compliance warning to explain or clarify some aspect of the scope or applicability of the Principles.³

II. The Compliance Warning

Today, the Accountability Program issues its second compliance warning to clarify that the OBA Principles are applicable and will continue to be enforced irrespective of the technology employed to collect and use consumer web surfing activity to serve interest-based ads.⁴ We also note that the Accountability Program’s existing body of public decisions and administrative

¹ The Accountability Program works closely with its sister accountability agent, the Direct Marketing Association (DMA), which resolves consumer and business complaints through its Corporate Responsibility Team, in conjunction with the DMA Committee on Ethical Business Practice.

² Enforcement of the Mobile Guidance will begin after companies have had the opportunity to put the new consumer choice tools currently under testing into operation.

³ See generally, “Accountability Program Issues First Industry-Wide Compliance Warning,” (“The Compliance Warning is a new tool that the Accountability Program will use to alert the advertising industry about its obligations”), available at <http://www.ascreviews.org/2013/10/accountability-program-issues-first-industry-wide-compliance-warning/>.

⁴ See OBA Principles, Definition G, defining OBA as the “collection of data from a particular computer or device regarding Web viewing behaviors over time and across non-Affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors.”

dispositions interpreting the Principles are generally applicable no matter by what technical means data for OBA is collected.⁵

III. Background

Digital advertising is a rapidly evolving industry where companies are constantly developing new technological tools and business models. The Principles were designed with that reality in mind to be flexible, functional and technologically agnostic. Given the constantly-evolving technologies and business models in the industry, the Principles had to be capable of application to any situation and any technology where consumers needed to be provided with transparency and control over the collection and use of their data for interest-based advertising.

Moreover, the OBA Principles were created in response to concerns that consumers had no way of knowing when their data was collected and used for personalized advertising and no way to exercise control over that use. The cornerstones of the OBA Principles—transparency through real-time notice and consumer control through an easy-to-use opt-out mechanism—were developed specifically to address these concerns. The core concerns about the use of alternative identification technologies are their lack of transparency to consumers and the absence of meaningful choice about whether such identifiers will be used to collect and deliver interest-based advertising. Providing transparency and consumer control are essential to address these issues.

The Accountability Program issues this compliance warning today in light of the changing landscape in personalized digital advertising. HTTP cookies have long been the predominant method used by the advertising industry to reach consumers with ads tailored to their interests. These small text files store a limited amount of data—a user ID hash, for example—and are stored in a specific directory the browser reserves for cookies, making them easy to locate, view or delete through common browser options. In the past few years, however, consumers have turned increasingly to a variety of different platforms and devices where cookies are not usable. These technological innovations have created new challenges and opportunities. The advertising industry has developed alternatives to the traditional HTTP cookie in order to reach consumers in this multi-platform, multi-device world with personalized advertisements likely to be of interest to them. As new “cookie-less” technologies increasingly replace the more familiar “cookies” in the delivery of personalized advertising across multiple screens, consumers must continue to receive real-time “enhanced” notice and an easy-to-use and effective opt-out mechanism.

Recent discussions about the development and use of alternative technologies such as Flash cookies, canvas fingerprinting and other “cookie-less” identification technologies have suggested that these technologies present novel consumer privacy issues that cannot be addressed through existing regulations and self-regulatory programs. We disagree.

⁵ The Accountability Program’s decisions are available at <http://www.asrcreviews.org/accountability-program-decisions/>. The Accountability Program’s administrative dispositions and closures are available at <http://www.asrcreviews.org/category/ap/accountability-program-administrative-dispositions/>. The Accountability Program’s compliance warnings can be found at <http://www.asrcreviews.org/category/ap/accountability-program-compliance-guidance/>.

As we will discuss below, the Accountability Program has spoken directly on this issue in a prior case.⁶ The Federal Trade Commission (FTC) and the Network Advertising Initiative (NAI) have also taken enforcement actions with respect to analogous issues. These decisions have made clear that companies using alternative identification technologies have the same obligations as companies using the more common “cookie” identification technology. We will look briefly at the FTC settlements and the NAI action before turning to the Accountability Program’s decision.

IV. Related Federal Trade Commission and Network Advertising Initiative Actions

The FTC has enforcement authority under Section 5(a) of the FTC Act to bring action where it finds “unfair or deceptive acts or practices in or affecting commerce.”⁷ The FTC has used its Section 5 authority in connection to what it considered deceptive uses of alternative identification technologies. For example, in 2011, the FTC settled with ScanScout, Inc., (ScanScout) which the FTC had reason to believe had used Flash cookies to circumvent the opt-out promise it made to consumers with respect to tracking.⁸ “The proposed settlement bars misrepresentations about the company’s data-collection practices and consumers’ ability to control collection of their data. It also requires that ScanScout take steps to improve disclosure of their data collection practices and to provide a user-friendly mechanism that allows consumers to opt out of being tracked.”⁹

Additionally, in 2013, the FTC settled with Epic Marketplace, Inc. (Epic Marketplace), which used a “history-sniffing” script to collect data on users’ web browsing habits for use in interest-based advertising without disclosing the practice in its privacy policy.¹⁰ The twenty-year consent decree prevents Epic Marketplace from employing history-sniffing scripts and making “misrepresentations about the extent to which they maintain the privacy or confidentiality of data from or about a particular consumer, computer or device, including misrepresenting how that data is collected, used, disclosed or shared” as well as “the extent to which software code on a webpage determines whether a user has previously visited a website.”¹¹

The FTC was not alone in taking action against Epic Marketplace. In its annual report for 2011, the Network Advertising Initiative (NAI) indicated that Epic Marketplace had violated the NAI Code and NAI policies and as a consequence, for three years, the NAI would require “Epic to undergo annual audits performed by an independent third party to help ensure that the technologies it uses for advertising purposes provide users an appropriate degree of transparency and control under the NAI Code; that history sniffing is not occurring, no history sniffing data

⁶ We also note that in 2013, the DAA convened a day-long industry conference to discuss alternate identifiers and promote understanding among participants that the DAA’s Principles encompass these technologies.

⁷ 15 U.S.C. § 45(a)(1)

⁸ *In the Matter of ScanScout, Inc.*, FTC File No. 102 3185. (Dec. 14, 2011)

⁹ Federal Trade Commission, *Online Advertiser Settles FTC Charges ScanScout Deceptively Used Flash Cookies to Track Consumers Online* (2011), <http://www.ftc.gov/news-events/press-releases/2011/11/online-advertiser-settles-ftc-charges-scanscout-deceptively-used> (last visited Aug 13, 2014).

¹⁰ *In the Matter of Epic Marketplace, Inc.*, FTC File No. 112 3182. (Mar. 19, 2013)

¹¹ Federal Trade Commission, *FTC Settlement Puts an End to “History Sniffing” by Online Advertising Network Charged With Deceptively Gathering Data on Consumers* (2012), <http://www.ftc.gov/news-events/press-releases/2012/12/ftc-settlement-puts-end-history-sniffing-online-advertising> (last visited Aug 13, 2014).

being collected, stored, or used by Epic’s systems; and that Epic otherwise is continuing to comply with NAI requirements.”¹²

V. The Accountability Program’s Guidance on the Use of Alternative Identification Technologies

In its 2012 BlueCava decision, the Accountability Program made clear that the OBA Principles are equally applicable to alternative identification technologies as to cookies used for OBA.¹³ BlueCava used its proprietary technology to determine the likelihood that multiple devices were associated with the same household. BlueCava explained how the technology worked in its privacy policy and provided consumers with an opt out. While the Accountability Program recognized BlueCava’s positive work to comply with the OBA Principles, the Accountability Program asked BlueCava to revise its privacy policy to clarify whether the opt-out mechanism it provided was effective across multiple devices or worked exclusively on the device from which a consumer exercised the option to opt out. BlueCava promptly clarified the point in its privacy policy, stating that the opt out was then only technically able to cover the device from which the consumer had exercised her choice.

While not required under the OBA Principles, the Accountability Program asked BlueCava whether it would be possible to develop a cross-device opt out. BlueCava voluntarily undertook to work on developing a solution to provide a multiple-screen opt out. It now offers its clients the option of a cross-screen opt out, thereby differentiating its products on the basis of its privacy capabilities and the seriousness of its compliance with privacy best practices.¹⁴

This illustrates the positive value of self-regulation. As the Accountability Program stated in the BlueCava decision and reiterates in this compliance warning:

*As technologies continue to evolve and raise new compliance issues, the Accountability Program will respond to ensure that the OBA Principles are preserved and can extend to meet these novel situations. Companies’ commitment to applying the OBA Principles to their new technologies will ensure that the OBA Principles continue to evolve along with technological advances. Technological innovation provides new challenges, but also can lead to innovative solutions that benefit consumers.*¹⁵

When companies develop new advertising technologies, they must be cognizant of the fact that the existing self-regulatory framework will follow them into these new frontiers. Development and testing processes should operate not only to produce innovative products, but also to incorporate “privacy by design,” including adherence to the requirements of the Principles.

¹² Network Advertising Initiative, 2011 Annual Compliance Report (Feb. 14, 2012).

¹³ In re: BlueCava, Inc. (May 2012) available at <http://www.asrcreviews.org/wp-content/uploads/2012/05/BlueCava-Decision-Final9.pdf> (hereinafter BlueCava Decision).

¹⁴ See <http://bluecava.com/platform/> (In its description of the benefits of using its products, Blue Cava includes “Privacy Friendly and Compliance,” stating: BlueCava takes a transparency and consumer choice focus on privacy, working with the top industry groups and associations. Cross-screen opt-out available.”)

¹⁵ BlueCava Decision.

Companies developing and implementing these technologies for OBA must provide effective enhanced notice, whether by adopting existing solutions or creating new ways to deliver enhanced notice on interest-based ads. Companies must also ensure that their OBA opt-out mechanism provides consumers with real choice, which may require linking their back-end technologies to existing opt-out mechanisms so that they will function seamlessly no matter what technology is being employed. These maxims are particularly important when employing cross-device identification technology and/or multiple means of collection for OBA.

Further, web publishers must be aware of the types of technologies employed by the third parties they allow to collect data for OBA on their websites. As with collection via HTTP cookies, when website publishers permit third parties to collect data for OBA using alternative identification technologies, they bear responsibility to provide enhanced notice on every page where that collection takes place and a disclosure of OBA practices that includes a compliant opt-out link that will work effectively with these cookie-less technologies.

Finally, today the Accountability Program also reminds companies that the MSD Principles, with their ban on using multi-site data for making crucial eligibility determinations, apply no matter how that data is gathered across sites.

The only questions left open for companies concern choosing how—not whether—to comply. If companies have questions about their responsibilities or are unsure how to implement compliant solutions, the Accountability Program encourages them to consult with us. A company that comes forward voluntarily to work out a reasonable compliance plan with us confidentially can avoid the risk of an inquiry and public decision.

VI. Conclusion

Companies engaged in online behavioral advertising as defined by the OBA Principles must adhere to the self-regulatory requirements provided therein without respect to the technologies they employ. Companies using alternate identifiers should provide the same level of transparency and choice to consumers as they would when using HTTP cookies. These self-regulatory principles build trust between consumers and online advertisers. When consumers understand interest-based advertising and are confident that their choices will be respected, they are more likely to respond favorably to personalized advertising. The Accountability Program believes that marketplace trust is essential to the success of e-commerce. Strong self-regulation helps build marketplace trust between businesses and consumers. By issuing this compliance warning today, the Accountability Program seeks to remind industry of its obligations and demonstrate that self-regulation can and will respond promptly and vigorously to ensure that in this era of rapid change, self-regulation will remain constant and unswerving.