



# Online Interest-Based Advertising Accountability Program



## COMPLIANCE WARNING

SUBJECT: February 1, 2017, Enforcement of Cross-Device Guidance

### **Introduction:**

The Online Interest-Based Advertising Accountability Program (Accountability Program) warns all first and third parties that starting today, February 1, 2017, the Accountability Program is enforcing the [Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices](#) (Cross-Device Guidance). The Cross-Device Guidance clarifies how companies who try to reach consumers across their various computers and mobile devices should provide them with notice and choice about IBA.

In recent years, consumers have increasingly begun to use multiple devices in their daily lives. As consumers move seamlessly across smartphone, tablet, laptop, and desktop, the IBA ecosystem has developed new ways of collecting and using data to serve IBA across these multiple devices. Cross-device IBA allows companies to learn about a consumer's interests on one device and show them ads relevant to those interests on other devices. Depending on the technology available to the company, the identity of the consumer or device is either "probabilistic," that is, based on a number of factors that link a user or related users who share devices, or "deterministic," that is, based on a user's sign-in or other method of self-identification across devices.

We note that these innovations in digital advertising have taken place in less than a decade. That is why self-regulation is so important. Self-regulation has the ability to respond quickly to technological and business change. Vigorously and independently enforced self-regulation can provide a strong, flexible framework to address consumer privacy concern in the dynamic digital marketplace.

### **Background:**

The original [Self-Regulatory Principles for Online Behavioral Advertising](#) (OBA Principles), released in 2009, brought transparency and consumer control to the desktop world of cross-website data collection and use. The OBA Principles were followed shortly by the [Multi-Site Data Principles](#) (MSD Principles) in 2011, which made clear that advertising data collected for IBA could not be used to determine eligibility for important benefits such as health care, insurance, or loans. As consumers migrated to the world of mobile devices, the advertising industry developed new technologies to identify devices for IBA, and the DAA responded with

guidance to industry on mobile IBA through the [Application of Self-Regulatory Principles to the Mobile Environment](#) (Mobile Guidance) in 2013. With the Cross-Device Guidance, the DAA has demonstrated that the principles of transparency and consumer control can be adapted to rapid technological advances.

The Accountability Program has already begun studying the practices of companies who engage in cross-device IBA, and we begin active enforcement today. It is our view that companies have had a commercially reasonable time—more than one year now—to study the Cross-Device Guidance and bring their operations into compliance with it. Companies whose websites, apps, and ad platforms are not in compliance with the Cross-Device Guidance should reach out to us confidentially immediately with any questions or serious and unforeseeable problems in meeting the compliance deadline to avoid a formal inquiry.

We remind all companies engaged in the online IBA space that compliance with the DAA’s body of Self-Regulatory Principles, including the Cross-Device Guidance, is enforced industry-wide. The Accountability Program expects *all parties across the digital advertising ecosystem* to work together to ensure that consumers have transparency and control as required under the DAA Principles. In accordance with our previous cases, we will accordingly hold all covered parties responsible for compliance.

With these general points in mind, we provide below an explanation of what responsibilities parties have under the Cross-Device Guidance.

### **Cross-Device Guidance:**

Looking broadly at the application of the principle of transparency as applied in the cross-device environment, we first look at how third parties should describe their cross-device IBA practices. When describing their IBA data collection and use practices, third parties that engage in cross-device IBA should explain that “data collected from a particular browser or device may be used with another computer or device that is linked to the browser or device on which such data was collected.”<sup>1</sup> This includes the collection and transfer of such data to another third party for its use in cross-app IBA. In short, third parties must ensure their privacy policies clearly explain the notion of cross-device IBA, how it is used, and crucially, as described below, the scope of any opt-out.

Second, the Cross-Device Guidance also explains how consumers’ choices not to participate in IBA should be treated in a cross-device context. As summarized by the DAA in a recent blog post, “[n]o browsing and usage data may flow *into* or *out of* that device/browser for the purposes of IBA” after the point where a consumer chooses to opt out.<sup>2</sup> Companies should not collect data from the opted-out device for use in IBA on a linked device; this includes transferring the data to another third party for its use in IBA. Companies also should not use data collected on a consumer’s other devices to serve IBA on the opted-out device. We think of the opted-out device

---

<sup>1</sup> *Cross-Device Guidance* at 3.

<sup>2</sup> Lou Mastria, *Cross-Device Guidance for DAA Principles: Enforcement Begins on Feb. 1, 2017*, <http://www.aboutads.info/blog/cross-device-guidance-daa-principles-enforcement-begins-feb-1-2017> (last visited Jan. 31, 2017).

as a “black hole” from which no data for IBA can escape and into which no IBA ads can go. Finally, we note that a consumer’s decision to opt out affects data collection and use *going forward*. Data collected from a device prior to opting out is not affected by the opt-out decision.

We once again remind all parties that if they operate a website, they are first parties. As our [First Party Enhanced Notice Compliance Warning](#)<sup>3</sup> and our dozens of cases<sup>4</sup> on this point have held, all first parties must provide proper notice and enhanced notice when companies are collecting data for IBA on their websites or apps. Specifically, first parties must provide an enhanced notice link on each page where such IBA activity occurs that takes consumers *directly* to a disclosure that describes this activity and provides information about opting out. In the cross-device context, first parties should be sure that the opt-out mechanism(s) to which they link in their IBA disclosures meet the standards of the DAA Principles, including the Cross-Device Guidance as described above.

To assist companies in understanding and implementing the Cross-Device Guidance, we wanted to raise several points of good practice:

- It is important that consumers understand cross-device IBA and have clear access to an easy-to-use mechanism by which to exercise choice. We therefore warn first and third parties that use a third-party provider to deliver notice and provide an opt out that it is their responsibility to provide an up-to-date, fully functioning link to the third-party provider that takes the consumer to their description of their IBA practices and their consumer control mechanism.
- The Cross-Device Guidance requires only that an opt out apply to the collection and use of IBA on the device on which the opt-out is provided. Not all companies currently have the technological capacity to provide an opt out across all devices. It could be misleading to claim to provide a broader opt out than a company is certain it can deliver. Moreover, there may be reasons that a particular consumer does not want an opt out to apply to all of her devices. Companies that have the technical capacity are, of course, free to offer an opt out from IBA across all devices associated with a particular identifier or individual. What is crucial is that the scope of any opt out be clearly explained. It is helpful to let consumers know how they can opt out of other devices that may be linked.
- We note that updates to websites to modify privacy policies may inadvertently cause links to break or content to be dropped, so we advise companies to check that the updates their IT teams make do not disturb current links or omit information as they implement any changes.
- Finally, we note that the Cross-Device Guidance applies to both the “deterministic” and “probabilistic” methods of cross-device IBA. Deterministic cross-device IBA is generally

---

<sup>3</sup> Available at <http://www.ascreviews.org/wp-content/uploads/2013/10/Accountability-Program-First-Party-Enhanced-Notice-Compliance-Warning-CW-01-2013.pdf> (last accessed Jan. 30, 2017).

<sup>4</sup> See, e.g., *In re: Answers Corporation* (38-2014, Oct. 28, 2014), *In re: Best Buy Co.* (39-2014, Oct. 28, 2014), *In re: Yelp* (40-2014, Oct. 28, 2014), *In re: TWiT, LLC* (46-2015, May 14, 2015), and *In re: The Hollywood Reporter, Inc.* (58-2015, Jan. 14, 2016).

accomplished when a user logs in to the same account—an email or social media account, for example—on more than one device. Because the consumer has concretely demonstrated that she uses each of these devices, companies can associate the activity among these devices.

Probabilistic cross-device IBA describes a set of techniques that allow companies to associate devices based on certain shared traits that seem to indicate the same person or close-knit group of people is using all of those devices. For example, a company may infer that two devices that are behind the same public IP address and which routinely visit a nearly-identical combination of obscure websites are likely to belong to the same person or household.

Once more, we invite companies with questions about their responsibilities under the Cross-Device Guidance to contact us right away.

### **Who We Are:**

The Accountability Program is one of the two accountability agents<sup>5</sup> charged by the DAA with enforcing the DAA’s Self-Regulatory Principles.

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 exercises its discretion to issue a public compliance warning to explain or clarify some aspect of the scope or applicability of the Principles.<sup>6</sup>

---

<sup>5</sup> The Accountability Program is an investigative unit of the advertising industry’s system of self-regulation and is administered by the Council of Better Business Bureaus. 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.

<sup>6</sup> 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/>.