I. Synopsis

The Digital Advertising Alliance's (DAA) Self-Regulatory Principles (DAA Principles) cover entities engaged in interest-based advertising (IBA) across websites or mobile applications (apps). Any operator of a website (a first party) that allows unaffiliated entities (third parties) to collect visitors' web browsing data for IBA.

1 The DAA's interest-based advertising principles consist of a suite of four documents: the Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles), the Self-Regulatory Principles for Multi-Site Data (MSD Principles), the Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance) and the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (Cross-Device Guidance) (collectively, the Principles). The full text of the Principles can be found at http://www.aboutads.info/principles.

2 The DAA Principles assign responsibilities to an entity based on its role in a particular situation. Thus, an entity can be a first party, third party, or service provider depending on the function it is performing. Website operators are first parties. OBA Principles Definition F at 10 (“A First Party is the entity that is the owner of the Web site or has Control over the Web site with which the consumer interacts and its Affiliates.”). See also Accountability Program, First Party Enhanced Notice Compliance Warning, CW-01-2013,

assets.bbbprograms.org/docs/default-source/daap/program-guidance/accountability-program-first-party-enhanced-notice-compliance-warning-cw-01-2013.pdf?sfvrsn=25e3af96_4. In the context of mobile applications, the first party is defined as the entity that owns or exercises control over the app, or its affiliates. Mobile app publishers are first parties under the Mobile Guidance. See Mobile Guidance Definition G at 7.

3 In the desktop context, third parties are entities that collect data for IBA from non-affiliate websites. See OBA Principles Definition J at 11 (“An entity is a Third Party to the extent that it engages in Online Behavioral Advertising on a non-Affiliate's Web site.”). In the mobile app context, the term “third party” refers to entities that collect data for IBA through non-affiliate
must provide visitors with notice and enhanced notice as prescribed in the Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles). Under the OBA Principles, third parties engaged in IBA must provide notice of IBA collection and provide visitors with a method to exercise choice over collection activities across sites and devices.

II. Company Status

Sonobi is an advertising technology developer and digital advertiser who engages in IBA collection across non-affiliate websites that it does not own or operate to build audience segments for digital advertising campaigns. As such, Sonobi meets the definition of “third party” for purposes of the DAA Principles.4

III. Inquiry

This case arises from a complaint indicating that consumers were unable to effectively opt out from Sonobi’s IBA collection even after using the industry-developed opt out tools provided by the DAA5 and Network Advertising Initiative (NAI).6 These tools can be used both to set opt-out preferences for participating advertisers and to check if a given advertiser is tracking the user across websites. After receiving the complaint, the Accountability Program checked the tracking status for Sonobi on both tools and discovered that cross-site tracking by Sonobi continued to occur even after an opt-out preference was set by a consumer. When reviewing the Sonobi privacy policy, the Accountability Program also discovered that Sonobi had not adopted a statement of adherence to the DAA Principles.

Based on the above review, the Accountability Program sent an inquiry letter to Sonobi explaining our concern that Sonobi’s advertising technology was not respecting opt-out signals, in violation of the DAA Principles.

IV. Issues Raised

A. Website data collection

1. Consumer control

Whether on desktop or mobile devices, third-party advertisers engaged in IBA must provide consumers with a means to opt out from IBA collection. The consumer

mobile apps, Mobile Guidance Definition N at 12 (“An entity is a Third Party to the extent that it collects Cross-App or Precise Location Data from or through a non-Affiliate’s application, or collects Personal Directory Data from a device.”).

4 Id.


control provision of the Cross-Device Guidance explains how opting out functions in the context of cross-device IBA. According to this provision, companies should not collect browsing or app usage data from the opted-out device for use in IBA on that device or 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 linked devices to serve IBA on the opted-out device. Companies are free to expand the scope of their opt outs to cover all devices linked to the device from which a consumer opts out. However, the Cross-Device Guidance does not require this expansive opt-out scope. Rather, companies may continue to treat opt outs as applying only to a particular browser or device. Whichever method a company chooses, it must be sure to clearly explain the scope of the opt out in its disclosure described under the transparency section of the Cross-Device Guidance so that consumers are apprised of the effect their opt-out decision will have. 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.

In this case, the consumer complaint alleged that Sonobi’s advertising technology would not respect the status of opt-out cookies set by the DAA and NAI tools. To test both tools, the Accountability Program set a Sonobi opt-out cookie and subsequently visited websites where Sonobi is known to engage in data collection for IBA purposes. Each time the Accountability Program visited one of these sites to test Sonobi’s ad tech—regardless of the opt-out method used—network traffic analysis and the opt-out tool tracking status indicator indicated that a Sonobi web server overwrote the existing opt-out cookie, replacing the consumer opt out with a user profile cookie and a brand-new unique identifier. This behavior, which ignored previously set opt-out cookies regardless of the opt-out method used, was observed across multiple tests using various configurations and devices.

Despite the presence of the Sonobi opt-out cookie, Sonobi servers consistently overwrote the consumer opt out with a new identifier. It therefore appeared that tracking for IBA purposes continued to occur despite the consumer’s exercise of choice not to participate in IBA. The Accountability Program also observed Sonobi passing the contents of the user profile cookie to other third-party companies known to engage in IBA through the use of cookie syncing servers, thereby disclosing a consumer’s unique identifier to other third parties even after the consumer had opted out of IBA collection. Finally, Sonobi’s privacy policy section that included a description of how to opt out of Interest-Based Advertising was missing the company’s statement of adherence to the OBA self-regulatory principles.

---

7 OBA Principles at 4.
8 Id., n.8.
9 Id. at 4 n.9.
V. Company response and analysis

In response to the Accountability Program’s inquiry letter, Sonobi immediately conducted a review of its compliance with the DAA Principles to identify areas in its protocols that needed strengthening.

Sonobi discovered an error in its advertising technology that affected the opt-out logic and resulted in Sonobi servers overwriting previously established opt-out preferences. Recent changes to the modularity of Sonobi’s advertising services made the cookie setting feature unaware of, and unable to respond to, existing opt-out signals. Because Sonobi’s servers could not identify the presence of an opt-out cookie on consumer devices, Sonobi’s advertising server would respond to web traffic from opted-out consumers by automatically generating a new user ID cookie and setting this cookie as a file on the consumer’s browser, using the same default logic that Sonobi servers use when a wholly new device interacts with Sonobi for the first time.

Sonobi corrected the error in their server’s response to opt-out cookies, and subsequently the Accountability Program found that Sonobi’s opt-out cookies operate properly, allowing users to set an opt-out preference that remains and prevents further collection by Sonobi regardless of subsequent browsing activity. Sonobi also added a statement of adherence to reflect the company’s commitment to the DAA Self-Regulatory Principles.

VI. Company statement

Sonobi promptly corrected the error and took action to ensure that, moving forward, its advertising servers would respect consumer opt-out cookies. Sonobi is committed to transparency and consumer choice, reflected by its expeditious action steps to rectify the error.

VII. Disposition of decision

Practices voluntarily corrected.