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, https://www.bbb.org/us/Storage/113/Documents/First-Party-Compliance-Warning-20131008.pdf. 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 mobile apps, Mobile Guidance Definition N at 12 (“An entity is a Third Party to the extent that
must provide visitors with notice and enhanced notice as prescribed in the Self-
Regulatory Principles for Online Behavioral Advertising (OBA Principles). Mobile
app publishers that authorize third parties to collect data through their apps for use
in cross-app IBA must provide users with notice and enhanced notice, as described in
the Application of Self-Regulatory Principles to the Mobile Environment (Mobile
Guidance).

II. Company Status

WhaleCo Inc. (Temu) is incorporated in Delaware, operates the Temu online
marketplace, and publishes the Temu website and mobile application. Since
beginning operations in September 2022, Temu’s mobile application has been one of
the top downloaded free applications on both the Android and iOS app stores.

III. Inquiry

As part of its routine monitoring and enforcement efforts, the Accountability
Program opens investigations based on consumer complaints regarding alleged
noncompliance with the OBA Principles.

This specific case arises from multiple consumer complaints claiming that Temu’s
website was not in compliance with the requirements of the Transparency Principle
of the OBA Principles.\(^4\) In response to the consumer complaint, the Accountability
Program visited the website www.temu.com to review Temu’s compliance with the
Principles. During its visit, the Accountability Program observed data collection by
third-party companies known to engage in IBA.

When the Accountability Program examined Temu’s website, we located a link in the
site footer labeled “Privacy policy and settings.”\(^5\) When we clicked on the Privacy
policy and settings link, it directed users to the top of the company’s Privacy &
Cookie Policy. After significant scrolling, we identified a description of third-party
IBA practices on the Temu site. Much further down the page, we also discovered a
broken hyperlink to the DAA-developed third-party IBA opt-out tool, which,
therefore, was not navigable. Temu’s policy did not include a statement of adherence
to the DAA Principles.

Under the Transparency Principle, Temu must provide a link—distinct from the
privacy policy link—on each webpage where third-party data collection for IBA
occurs on browsers. An enhanced notice link must, unlike the Temu website’s

\(^4\) See OBA Principles § II.B. at 13–14.
privacy policy link, take users directly to its IBA disclosure and a method to opt-out of third-party IBA.

The Accountability Program also examined Temu’s mobile application. We observed data collection by third-party companies known to engage in IBA. When the Accountability Program examined the Temu mobile app we discovered that, similar to the Temu website, enhanced notice for mobile applications was not present in any of the times or places prescribed in the Transparency Principle of the DAA Mobile Guidance.6

Based on the above review, the Accountability Program sent an inquiry letter to Temu explaining the compliance issues it had found on its website.

IV. Issues Raised

A. Website data collection

1. Enhanced notice of website data collection for IBA

First-party duties under the OBA Principles are set out in section II.B. According to this section, if first parties allow third parties to collect visitors’ browsing data for use in IBA on their websites, or if they transfer such data to third parties for tailoring ads on non-affiliate websites, they must provide consumers with appropriate transparency and an opportunity to exercise control over IBA.7 A first party must include a disclosure somewhere on its website that describes the IBA activity occurring there.8 This disclosure must contain either a link to an industry-developed consumer choice page (such as http://aboutads.info/choices) or a list of every third party conducting IBA activity on the first-party website.9 Additionally, a first party must state its adherence to the DAA Principles on its website.10

Most significantly, the OBA Principles require first parties to provide consumers with real-time “enhanced notice” when third parties are collecting or using data for IBA on a first party’s website. This real-time indicator must be in the form of a “clear, meaningful, and prominent” link that directs consumers to the first party’s IBA

---

6 See Mobile Guidance § III.A.3. at 17.
7 OBA Principles § II.B. at 13–14.
8 Id.
9 Id. We note that when first parties choose to list third parties individually, the Commentary to the Consumer Control Principle instructs companies that “choice should be available from the Third Party(s) disclosure linked from the page where the Third Party is individually listed.” OBA Principles Commentary at 35.
disclosure, not just to the top of a privacy policy.\textsuperscript{11} In addition, this link must be distinct from the company’s privacy policy link and must appear on every page where data collection or use for IBA occurs on the first party’s website.\textsuperscript{12} The link may be provided directly by the first party or by one of the third parties active on its website.\textsuperscript{13}

Enhanced notice provides consumers with two benefits. First, it informs consumers of the fact that third parties are engaged in IBA on a website. Second, by linking directly to a disclosure that describes the IBA activities occurring on that website and providing a method by which consumers can exercise choice, enhanced notice serves as a bridge to relevant information consumers need at precisely the time they need it. By drawing attention to this otherwise invisible background activity in real time, explaining it in plain language, and providing one or more choice mechanisms, enhanced notice helps consumers understand IBA and make choices about the use of their data for IBA.

\textbf{B. Mobile data collection}

The Mobile Guidance adapts the desktop-oriented rules of the OBA Principles to the mobile world, including the core requirements to provide transparency and consumer control of IBA. In particular, when first parties permit third parties to collect data through their apps for use in IBA, they must provide enhanced notice and choice about such third-party data collection for IBA.\textsuperscript{14}

\textbf{1. First-party cross-app enhanced notice requirement}

According to section III.A.(3) of the Mobile Guidance, first parties that affirmatively authorize a third party to collect or use cross-app data for IBA must provide a clear, meaningful, and prominent link to a disclosure that (1) describes the third-party collection, (2) points to a choice mechanism/setting or lists all third parties with links to their opt outs, and (3) contains a statement of adherence to the DAA Principles.\textsuperscript{15} The enhanced notice link must be provided prior to download (e.g., in the app store on the application’s page), during download, on first opening of the app, or at the

\textsuperscript{11} \textit{OBA Principles} Commentary at 32 (“The Principles also state that the Web sites at which Third Parties are collecting data for Online Behavioral Advertising purposes should include a new clear, meaningful, and prominent link on their Web sites when Third Parties do not provide the notice described in II.A.(2)(a). This would link from the Web page where data is collected to specific language in a disclosure. If the disclosure language is in the privacy notice, the link should go directly to the relevant section of the privacy policy where the disclosure is located and not just generally to the privacy policy.”).

\textsuperscript{12} \textit{Id.} at 31.

\textsuperscript{13} \textit{First Party Enhanced Notice Compliance Warning} at 3.

\textsuperscript{14} \textit{Mobile Guidance} at 17.

\textsuperscript{15} \textit{Id.}
time cross-app data is first collected, and in the application’s settings or any privacy policy.\textsuperscript{16}

These enhanced notice requirements make information about privacy more accessible to users so they can make an informed decision about whether to participate in data collection and use for IBA. The enhanced notice link must go directly to the place where the app explains its IBA practices. Moreover, the link must be provided at or before the moment a user’s engagement with the app results in third-party data collection for IBA. This process provides a conspicuous, accessible, and meaningful disclosure to the consumer at the time it is most useful to them. As such it is a dramatic improvement on the past practice of simply placing the information in a dense privacy policy. It also requires that the company’s disclosure explain to consumers how they can opt out of IBA, including providing links to easy-to-use opt-out mechanisms like the DAA’s AppChoices tool.\textsuperscript{17}

V. Company response and analysis

In response to the Accountability Program's inquiry letter, Temu immediately conducted a comprehensive review of its compliance with the DAA Principles in order to identify any areas in its compliance protocols that needed strengthening. The company worked diligently to find comprehensive solutions to each issue and consulted with the Accountability Program on its plan to come into compliance with the DAA Principles, as explained below.

\textbf{A. Enhanced Notice of website data collection for IBA}

To meet its enhanced notice obligations under the OBA Principles, Temu edited its website footer to add an “Ad Choices” link at the bottom of each webpage on the site. Because a “Sign In” popup had previously prevented users from accessing footer

\textsuperscript{16} Id. We note that where the third party is unable to provide enhanced notice and choice in an app, the first party should work with the third party to ensure that such notice and choice are provided. See id. § III.B.(1) at 18-19. Compare Accountability Program, Compliance Warning, https://assets.bbprograms.org/docs/default-source/daap/program-guidance/accountability-program-first-party-enhanced-notice-compliance-warning-cw-01-2013.pdf?sfvrsn=25e3af96_4&_ga=2.236318813.106136300.1690986513-1162211555.1678714684&_gl=1*12nm72*_ga*MTE2MjIxmTU1NS4xNjc4NzE0Njg0*_ga_FX P6NWPNYM*MTY5MDk4NjUxMy41Mi4wLjE2OTA5ODY1NTQuMTkuMC4wLjA._ga_DG10F MY2E3*MTY5MDk4NjUxMy41Mi4wLjE2OTA5ODY1NTQuMC4wLjA.*_ga_BM4RBEEQ37*MTY5MDk4NjUxMy41Mi4wLjE2OTA5ODY1NTQuMC4wLjA at 2 (“Both the third party and the first party share responsibility for provision of enhanced notice. Because the third party which is collecting the data generally has no direct means to provide notice and choice on the website where its data collection is occurring, providing just-in-time notice of collection and an opt out requires cooperation between the third party engaged in the collection and the first party on whose website such collection is permitted.”).

\textsuperscript{17} Digital Advertising Alliance, Download the AppChoices Tool - Now with 'Do Not Sell' Enhancements, https://youradchoices.com/appchoices (last visited Jan. 12, 2020).
links on mobile browsers, Temu moved the popup to ensure users on any browser – whether they were signed in or not – have the ability to click on the Ad Choices link.

This “Ad Choices” link takes users directly to the top of a newly edited privacy policy section titled “Interest-based Advertising.” Within this section, Temu placed all three elements of enhanced notice, namely (1) a description of Temu’s third-party IBA practices, (2) a link to industry-developed IBA opt-out tools, and (3) a statement of adherence to the DAA Principles.

B. Compliance with cross-app data collection requirements

Temu’s authorization of third-party collection of unique identifiers for IBA in its mobile app triggered compliance responsibilities under the first-party cross-app provisions of the Mobile Guidance.

The cross-app provisions of the Mobile Guidance prescribe particular times and locations where consumers can receive enhanced notice that directs them to a compliant IBA disclosure. The link should appear either before or concurrent with the initial collection of data for IBA. One means for providing enhanced notice before collection occurs is to do so through a link on the app’s listing in an app store. Where possible, this can be done through a dedicated enhanced notice link, but this is not always the case. The Mobile Guidance recognizes that app stores may allow only a finite set of links dedicated to specific resources, such as company websites and privacy policies. The flexibility of the Mobile Guidance allows app publishers to use the dedicated privacy policy link as its enhanced notice link where necessary.

To do so, app publishers must place an IBA disclosure or a link to a disclosure at the top of the privacy policy linked from the app store. This ensures that when a user taps on a privacy policy link in an app store listing, they are directed immediately to relevant information about IBA and an opt-out mechanism.

To resolve its issues under the enhanced notice provisions of the Mobile Guidance, Temu made substantial changes to ensure IBA disclosures were accessible to users in places proscribed by the Mobile Guidance. Temu added language at the top of its

---

18 Mobile Guidance § III.A.(3) at 17. See also In re Sega (65-2016), July 14, 2016; In re Spinrilla (61-2016), May 4, 2016; In re Bearbit Studios (62-2016), May 4, 2016; In re Top Free Games (63-2016), May 4, 2016.

19 Id. § III.A.(3) at 17.

20 Commentary. Id. § III.A.(3) at 18 (“Where a Third Party elects to satisfy Section III.A.2.ii.1 or a First Party elects to satisfy Section III.A.3.a by providing a link prior to installation through an application market that does not permit active links, the entity satisfies this Principle if it provides an active link to a privacy policy that contains the disclosure described in Section III.A.1 and directs consumers to the relevant section of the privacy policy where the disclosure is located.”).

21 Id. (allowing a jump link near the top of a privacy policy to direct consumers to an IBA disclosure where app stores do not allow active enhanced notice links).
privacy policy that reads “For information about interest-based advertising and your choices, click here” and provided a jump link that takes users to the aforementioned Interest-based Advertising section of the privacy policy. By doing so, Temu ensured that users could easily access this information from the application store pages once a user clicks on the app store privacy policy link.

In previous instances of the Temu mobile app, Temu did not display any in-app privacy settings to users until they created an account. To ensure enhanced notice was provided in-app to all users, Temu now displays a privacy tab under the settings page regardless of login status. On Android devices, Temu also added an in-application “Ad Choices” link to its privacy settings page. This “Ad Choices” link provides enhanced notice under the DAA Mobile Guidance and ensures that users on the Android platform can easily reach the Interest-Based Advertising section of the privacy policy directly from Android mobile application’s settings.

On the iOS platform, Temu removed third-party IBA collection from its mobile application altogether. When the Accountability Program first opened an inquiry into Temu’s IBA practices, the iOS Temu mobile application used a third-party software development kit (SDK) from a company known to engage in IBA as an analytics provider, an advertising partner, and as a service provider for single sign on. This third-party SDK was previously allowed to collect information that could be used to serve interest-based advertising to Temu users across other sites and applications.

To meet its obligations under both the DAA Principles and the Apple App Tracking Transparency framework, Temu took steps to change how the SDK was implemented on its iOS mobile application. These changes preserve the consumer’s ability to log in using single sign on for the Temu iOS mobile application; however, the SDK provider will no longer receive information from the iOS mobile application that can be used for interest-based advertising.

VI. Company statement
Consistent with Temu’s commitment to user privacy and transparency, we are proud to adhere to the DAA Principles. We work actively with the Digital Advertising Accountability Program to continuously enhance our disclosures about online behavioral advertising. We highly value the collaboration with the Program, as it plays a significant role in ensuring transparency and assuring users of the responsible management of their information.

VII. Disposition of decision
Practices voluntarily corrected.