

BBB NATIONAL PROGRAMS

***DIGITAL ADVERTISING
ACCOUNTABILITY PROGRAM***

DIGITAL ADVERTISING
ACCOUNTABILITY PROGRAM,
Challenger,

SHOPRUNNER, INC.,
Company.

Case No. 144-2025
Filed May 28, 2025

FINAL DECISION

I. Synopsis

The Digital Advertising Alliance’s (DAA) Self-Regulatory Principles (DAA Principles)¹ cover entities engaged in interest-based advertising (IBA) across websites or mobile applications (apps). Any operator of a website (a first party)² that allows unaffiliated entities (third parties)³ to collect visitors’ web browsing data for IBA 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).

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://assets.bbbprograms.org/docs/default-source/daap/program-guidance/accountability-program-first-party-enhanced-notice-compliance-warning-cw-01-2013.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 it collects Cross-App or Precise Location Data from or through a non-Affiliate’s application, or collects Personal Directory Data from a device.”)

II. Company Status

ShopRunner, Inc. is an e-commerce platform that connects millions of consumers to over 100 brands. In December 2020, FedEx announced that it had acquired ShopRunner to further expand e-commerce offerings to consumers.⁴ ShopRunner publishes the shoprunner.com website, as well as the iOS and Android ShopRunner mobile applications. As the publisher of online products that allow third-party advertisers to collect user browsing information for IBA purposes, ShopRunner is a first party under the DAA Principles.⁵

III. Inquiry

As part of its enforcement efforts, the Accountability Program opens investigations based on its own digital marketplace monitoring as well as consumer complaints regarding alleged noncompliance with the OBA Principles.

This specific case arises from routine monitoring. The Accountability Program visited the website www.shoprunner.com to review its conformance to 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 web pages on the ShopRunner website, we located a footer labeled “Policies” that directed users to ShopRunner’s privacy policy. The IBA information was contained in section 5 of the privacy policy, titled “Your Choices and Privacy Rights,” providing a brief description of third-party collection and links for DAA-developed third-party IBA opt-out tools. However, there was no separate and distinct link directing users to an IBA disclosure; such a link, known as “enhanced notice,” is required by the Transparency Principle of the OBA Principles (Section II.B). Additionally, the Accountability Program did not find a statement of ShopRunner’s adherence to the DAA Principles, which is also required under section II.B. of the OBA Principles.

Under the DAA Transparency Principle, ShopRunner 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 ShopRunner website’s 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 ShopRunner’s mobile application and observed third-party IBA-related data collection. Similar to the ShopRunner website, enhanced notice was not present in any of the times or places prescribed in the Transparency Principle of the DAA Mobile Guidance.⁶

⁴ FedEx, *FedEx to Acquire ShopRunner to Expand E-Commerce Capabilities*, <https://newsroom.fedex.com/newsroom/global/fedex-to-acquire-shoprunner-to-expand-e-commerce-capabilities>.

⁵ *OBA Principles*, Definitions §F. First Party.

⁶ *See Mobile Guidance* § III.A.3. at 17.

Based on the above review, the Accountability Program sent an inquiry letter to ShopRunner explaining the compliance issues it had found on ShopRunner’s websites and mobile applications.

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 disclosure, not just to the top of a privacy policy.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.¹² The link may be provided directly by the first party or by one of the third parties active on its website.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,

⁷ *OBA Principles* § II.B. at 13–14.

⁸ *Id.*

⁹ *Id.* If 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.

¹⁰ *OBA Principles* § II.B. at 13–14.

¹¹ *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.”).

¹² *Id.* at 31.

¹³ *First Party Enhanced Notice Compliance Warning* at 3.

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.

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.¹⁴

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.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 time cross-app data is first collected, **and** in the application's settings or any privacy policy.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 significant improvement on the past practice of simply placing the information in an often-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.¹⁷

¹⁴ *Mobile Guidance* at 17.

¹⁵ *Id.*

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.bbbprograms.org/docs/default-source/daap/program-guidance/accountability-program-first-party-enhanced-notice-compliance-warning-cw-01-2013.pdf> 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.”).

¹⁷ Digital Advertising Alliance, *Download the AppChoices Tool - Now with 'Do Not Sell' Enhancements*, <https://youradchoices.com/appchoices>.

V. Company response and analysis

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

A. *Enhanced Notice of website data collection for IBA*

To meet its enhanced notice obligations under the OBA Principles, ShopRunner added a website footer link titled “Interested based ads” that takes users directly to the IBA section of the privacy policy, titled “5. Your Choices and Privacy Rights.”

The above-mentioned section now includes all elements of DAA enhanced notice together, namely (1) a description of third-party IBA practices, including through descriptions of web tracking technologies used on ShopRunner’s digital properties, (2) a link to, and description of, industry-developed IBA opt-out tools, and (3) a statement of adherence to the DAA Principles.

B. *Mobile data; Compliance with cross-app data collection requirements*

ShopRunner’s authorization of third-party collection of unique identifiers for IBA in its iOS and Android mobile apps 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.¹⁸ The link should appear either before or concurrent with the initial collection of data for IBA.¹⁹ 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.²⁰ 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.²¹ This ensures that when users tap 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, ShopRunner made considerable changes to ensure IBA disclosures were accessible to

¹⁸ *Mobile Guidance* § III.A.(3) at 17.

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.*

users in places prescribed by the Mobile Guidance. First, the top of the ShopRunner privacy policy now contains a sentence with the following information: “Learn more about Interest-based Advertising and your Ad choices [here](#).” The included link redirects users to the IBA section of the privacy policy, titled “5. Your Choices and Privacy Rights.” Thus, users who click on the “Privacy Policy” link in the mobile app settings page can easily access information about IBA and their opt-out options.

ShopRunner’s iOS and Android app store listings both include privacy policy links that direct users to the top of ShopRunner’s privacy policy webpage, and further redirects users to the IBA section, as described in the previous paragraph. By doing so, users can easily access IBA information from the application store pages, through the app store privacy policy link.

VI. Company statement

At ShopRunner, a FedEx subsidiary, we are committed to delivering a seamless online experience, grounded in the core principles of privacy, transparency, and customer trust. We welcomed the opportunity to voluntarily collaborate with the Digital Advertising Accountability Program and applaud their dedication to promoting industry best practices. We appreciate their acknowledgement that we are compliant with the DAA Principles.

VII. Disposition of decision

Practices voluntarily corrected.

Digital Advertising Accountability Program