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

¹ The DAA Principles include a suite of four documents related to interest-based advertising which may be read in full at http://www.aboutads.info/principles. The relevant documents are titled: Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles), Self-Regulatory Principles for Multi-Site Data (MSD Principles), Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance), and Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (Cross-Device Guidance). The DAA also maintains a set of self-regulatory principles dedicated to political advertising, the Application of the Self-Regulatory Principles of Transparency & Accountability to Political Advertising, which are unrelated to this decision.

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, http://www.asrcreviews.org/wp-content/uploads/2013/10/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
collect visitors’ web browsing data for IBA must provide visitors with notice and enhanced notice as prescribed in the 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 Mobile Guidance.

COMPANY STATUS

Johnson & Johnson Consumer Inc. (J&J) is a company that provides over-the-counter pharmaceutical products. The company is headquartered in New Brunswick, NJ.

INQUIRY

This case arises from a consumer complaint alleging that the website for the skin care product Neutrogena allowed third parties to collect data for IBA (https://www.neutrogena.com/) without providing sufficient notice and choice to these users as required under the DAA Principles. In response to the complaint, the Accountability Program reviewed the Neutrogena website, where we observed data collection by a number of third-party companies known to engage in IBA. We then initiated a full review of J&J’s compliance with all applicable requirements of the DAA Principles. Below, we describe our examination in detail.

I. Desktop data collection review

The Accountability Program examined the Neutrogena website for an enhanced notice link, which is required by the OBA Principles, but we could not locate such a link. We then examined several other J&J websites to determine if the company had provided these types of links to visitors on its other web offerings. During our review, we noted that the J&J sites only included footer links to each site’s “Privacy Policy” page and either a “Terms of Use” or “Legal Notice” page. We could find no link that was distinct from a general privacy policy link that took users directly to a disclosure about IBA.

We then manually searched the Neutrogena and the other J&J websites’ privacy policy documents for a description of third-party data collection occurring on these websites that would satisfy the notice requirement of the OBA Principles. Neutrogena’s privacy disclosure appeared to describe third-party IBA activity under the heading “Online behavioral advertising,” nested under a section entitled “Passive Information Collection and Use.” However, we were unable to locate a link to an opt-out mechanism in this privacy policy or any of the other disclosures on the

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.”).

4 Mobile Guidance Definition D at 5 (“Cross-App Data is data collected from a particular device regarding application use over time and across non-Affiliate applications. Cross-App Data does not include Precise Location Data or Personal Directory Data.”).


Neutrogena website. The other J&J disclosures reviewed by the Accountability Program also lacked links to any opt-out mechanism, with the notable exception of the privacy policy for J&J’s Zyrtec brand. Moreover, we could not find a statement of the company’s adherence to the DAA Principles in any of the J&J privacy documents we reviewed.

II. Mobile data collection review

The Accountability Program examined J&J’s mobile app for its Zyrtec product, entitled ZYRTEC AllergyCast (Zyrtec app).7 We noted that this mobile app appeared to send information to third parties that may engage in IBA. Under the Mobile Guidance, third-party collection of cross-device data (including unique device IDs)8 through a mobile app for purposes of IBA may trigger first-party transparency requirements similar to those in the web context.

Following our review, the Accountability Program sent an inquiry letter to J&J detailing these issues and explaining the requirements of the DAA Principles.

ISSUES RAISED

I. 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.9 A first party must include a disclosure somewhere on its website that describes the IBA activity occurring there.10 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.11 Additionally, a first party must state its adherence to the DAA Principles on its website.12

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

---

9 OBA Principles § II.B. at 13–14.
10 Id.
11 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.
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{14} The link may be provided directly by the first party or by one of the third parties active on its website.\textsuperscript{15}

Enhanced notice provides consumers with two benefits. One, it informs consumers of the fact that third parties are engaged in IBA on a website. Two, 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.

II. Enhanced notice of mobile data collection for IBA

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{16}

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, \textbf{and} (3) contains a statement of adherence to the DAA Principles.\textsuperscript{17} 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, \textbf{or} at the time cross-app data is first collected, \textbf{and} in the application’s settings or any privacy policy.\textsuperscript{18}

\textsuperscript{13} \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{14} \textit{Id.} at 31.

\textsuperscript{15} First Party Enhanced Notice Compliance Warning at 3.

\textsuperscript{16} Mobile Guidance at 17.

\textsuperscript{17} Id.

\textsuperscript{18} 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. \textit{See id.} § III.B.(1) at 18-19. Compare Accountability Program, Compliance Warning, http://www.ascreviews.org/wp-content/uploads/2013/10/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.”).
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 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.

COMPANY RESPONSE AND ANALYSIS

I. Enhanced notice of website data collection for IBA

J&J responded to the Accountability Program inquiry by conducting a thorough review of its compliance with the DAA Principles. The company worked with the Accountability Program to revise its privacy disclosures and pledged to implement the Accountability Program’s recommendations in order to make its entire suite of websites compliant with the DAA Principles. The company added to the Neutrogena website an enhanced notice link labelled “AdChoices” which includes the DAA’s AdChoices Icon. When clicked, this link directs users to an updated section of the Neutrogena privacy policy which includes a disclosure about third-party IBA occurring on the website and a link to the DAA’s WebChoices page (http://aboutads.info/choices) and the Network Advertising Initiative’s Consumer Opt-Out Page (http://optout.networkadvertising.org/?c=1). J&J also updated the websites of several of its other offerings to include an enhanced notice link, and the company indicated to the Accountability Program that it aimed to ensure that all J&J websites that allowed IBA would implement the Accountability Program’s recommendations in order to make them compliant by the end of 2019. The Accountability Program found that this timeline was commercially reasonable and indicated it would retain jurisdiction on J&J’s case until all updates were completed.

II. Enhanced notice of mobile data collection for IBA

The Mobile Guidance prescribes particular times and locations where consumers can receive enhanced notice that directs them to a compliant IBA disclosure. The link should appear either

19 The Accountability Program notes that if the first party’s enhanced notice link uses the DAA’s AdChoices Icon and DAA approved wording, then it may serve independently as a site’s statement of adherence to the DAA Principles. See OBA Principles Commentary at 30 (“Finally, this Principle requires that all entities indicate adherence to these Principles in their notice. This Principle can be satisfied either by wording or the logo/icon of a self-regulatory accountability program. Taken together, these mechanisms for clearly disclosing and informing the public and consumers about data collection and use practices will significantly enhance the transparency of Online Behavioral Advertising practices and address certain perceived gaps in current practices.”) See also In re: Yelp, Inc. (40-2014), October 28, 2014 at 3.

20 J&J chose to license the AdChoices Icon and used it along with a recommended phrase for the link, “AdChoices.” Together, these modifications constitute the company’s statement of adherence. Id.

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, J&J committed to adding to the top of the privacy policy for its Zyrtec app a jump link which directs to language describing mobile IBA and a link to the DAA’s AppChoices app. J&J pledged to push this enhanced notice implementation across its entire suite of apps and committed to full compliance for its mobile apps by the end of 2019. The Accountability Program found this timeline commercially reasonable and accepted J&J’s commitment.

CONCLUSION

Today’s case again highlights the responsibility of publishers to provide consumers with enhanced notice of background data collection for IBA—whether this collection occurs in through the mobile apps or the traditional web environment. When publishers control and operate a significant number of mobile and web properties, this responsibility is amplified. Brands that enjoy massive consumer audiences and employ the technologies that facilitate IBA must honor consumer privacy and provide their website visitors and app users with transparency and choice about data collection.

When contacted by the Accountability Program, J&J recognized its position in the market and its obligations to consumers, and it quickly furnished the program a full list of its web and mobile app products. The company pledged to implement the Accountability Program’s recommendations in order to achieve compliance with the DAA Principles across all of these offerings and is on track to completion, with more than 70 websites already complete. The Accountability Program thanks J&J for its commitment to consumer privacy and industry self-regulation.

22 Id. § III.A.(3) at 17.
23 Id. Commentary at § 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.”).
24 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).
COMPANY’S STATEMENT

J&J strives to provide our customers with transparency and choice consistent with legal and self-regulatory requirements. We appreciate the Accountability Program for bringing this matter to our attention.

DISPOSITION OF DECISION

Practices voluntarily corrected, jurisdiction retained until all website and mobile app updates complete.

Jon M. Brescia  
Vice President  
Digital Advertising Accountability Program