

BBB NATIONAL PROGRAMS, INC.

DIGITAL ADVERTISING ACCOUNTABILITY PROGRAM

FORMAL REVIEW

Case Number: 111-2020

)
<u>COMPANY:</u>)
Mammoth Media, Inc.)
)
)
<u>CHALLENGER:</u>)
Digital Advertising)
Accountability Program)
)
)

DECISION

DATE: April 23, 2020

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). Mobile app publishers² that authorize third parties³ to collect data through their apps for

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 DAA also maintains a set of self-regulatory principles dedicated to political advertising which is not at issue in this case. The full texts of the Principles can be found at <http://www.aboutads.info/principles>. For a list of Accountability Program decisions, please see <https://ascreviews.org/accountability-program-decisions/>

² In the context of mobile applications, a “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 (“A First Party is the entity that is the owner of an application, or has Control over the application, with which the consumer interacts, and its Affiliates.”).

³ 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

use in cross-app⁴ IBA must provide users with notice and enhanced notice, as described in the Mobile Guidance. Additionally, if a company allows third parties to collect precise location data⁵ for IBA, it must provide users with the opportunity to consent to this collection, in addition to standard notice and enhanced notice of this fact.

COMPANY STATUS

Mammoth Media, Inc. (Mammoth) is a company that publishes entertainment apps focused on Generation Z audiences.⁶ The company publishes the social media mobile app Wishbone and the storytelling app Yarn, available on the Android and iOS operating systems.⁷ Mammoth is headquartered in Santa Monica, California.

INQUIRY

This case arises from the Accountability Program’s regular monitoring of mobile applications. The Accountability Program identified the Wishbone and Yarn apps and began reviewing them for compliance with the Mobile Guidance. The Accountability Program first installed the iOS and Android versions of the apps on our test devices and was able to capture and inspect data packets being transmitted from the applications.

i. Cross-app data review

Through analysis of network traffic generated from the apps, we observed third parties collecting cross-app data likely for IBA. Specifically, we noted the collection of Android’s Advertising ID (AAID or IFA) and Apple’s Identifier for Advertising.⁸ This prompted us to examine Mammoth’s compliance with the cross-app provisions of the Mobile Guidance.

To assess Mammoth’s compliance with the mobile enhanced notice requirement, the Accountability Program first examined the privacy policy links on the apps’ listings in the

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.”).

⁵ *Mobile Guidance* Definition K at 9 (“Precise Location Data is data obtained from a device about the physical location of the device that is sufficiently precise to locate a specific individual or device.”).

⁶ See generally Mammoth, *The Mobile Entertainment Studio*, <https://mammoth.la/> (last visited Nov. 12, 2019).

⁷ Apple App Store, *Wishbone – Compare Anything*, <https://itunes.apple.com/us/app/wishbone-compare-anything/id836071680?mt=8> (last visited Aug 29, 2019). Apple App Store, *Yarn – Chat & Text Stories*, <https://itunes.apple.com/us/app/yarn-chat-text-stories/id1195233335?mt=8> (last visited Nov. 12, 2019). Google Play Store, *Wishbone – Compare Anything*, https://play.google.com/store/apps/details?id=com.science.wishboneapp&hl=en_US (last visited Nov. 12, 2019). Google Play Store, *Yarn – Chat Fiction*, https://play.google.com/store/apps/details?id=com.science.yarnapp&hl=en_US (last visited Nov. 12, 2019).

⁸ IAB Mobile Marketing Center of Excellence, *Mobile Identity Guide for Marketers*, June 2017, at 4, <https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf> (“The most prevalent Advertising Identifiers today offering the scale needed for marketing purposes are the ... IDFA [and] AAID.”).

Google Play and Apple App Stores. These links directed us to the top of a privacy policy document⁹ for Mammoth’s apps.¹⁰ However, these links did not function as enhanced notice links, because they did not take us directly to a disclosure that describes the third-party IBA activity Mammoth allows through its mobile app offerings.¹¹ We could find no other links that would serve as enhanced notice under the Mobile Guidance.

Review of privacy policy linked from app stores

The Accountability Program looked further to determine if Mammoth had provided any disclosure of third-party data collection for IBA taking place through the Wishbone or Yarn apps and examined Mammoth’s privacy policy for such a disclosure. There, we located a discussion of third-party advertising that takes place through Mammoth’s products and services, and links to the industry-developed pages www.aboutads.info/choices and www.networkadvertising.org/choices:

We engage certain third-party service providers to serve advertisements on our behalf across the Internet and to provide analytics services. These entities may utilize Cookies or other similar technologies (including within the ads) to collect anonymous information from you such as your device identifiers and IP address, web browser, actions you take relating to the ads, any links you click on, and conversion information. This information may be used by us, our service providers and their clients in aggregated form to, among other things, analyze and track aggregated data, determine the popularity of certain content or products, measure the effectiveness of ad campaigns, determine the proper amount of repeat views of a given ad, and deliver advertising and content targeted to your interests on our platform and other websites (also known as “interest-based advertising”). These service providers are prohibited from collecting any Personal Data from you and we do not share any of your Personal Data with them.

To learn more about advertising networks and interest-based advertising, visit the Digital Advertising Alliance at www.aboutads.info/choices or the Network Advertising Initiative at www.networkadvertising.org/choices.¹²

While the Accountability Program recognized that Mammoth provided links to these industry-developed pages, we noted that the company did not provide clear language in its privacy policy explaining to users how they can opt out of mobile IBA by visiting these sites. We also could not locate a statement of adherence to the DAA Principles during our review of this privacy policy.

¹⁰ Mammoth, *Privacy Policy* (Jan. 19, 2019), http://d3ds02ejfx7ezp.cloudfront.net/ui/wb_pp.pdf [perma: <https://perma.cc/J5XU-X6NF>].

¹¹ *Mobile Guidance* Commentary to § III.A.(3) at 18 (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).

¹² Mammoth, *Privacy Policy* (Jan. 19, 2019), http://d3ds02ejfx7ezp.cloudfront.net/ui/wb_pp.pdf [perma: <https://perma.cc/J5XU-X6NF>].

Review of privacy policy linked from company website

The Accountability Program then located an alternative version of Mammoth’s privacy policy, which was accessible through Mammoth’s website (www.mammoth.la) but not linked from the Wishbone or Yarn app pages in the app stores.¹³ We noted that this website privacy policy provided somewhat clearer instructions to users for opting out of mobile IBA:

(b) Opt-out of Ad Tracking. You can opt out of the collection and use of your information for ad targeting by going to <http://www.aboutads.info/choices> or <http://www.youronlinechoices.eu/> to limit collection through the Site or by configuring the settings on your mobile device to limit ad tracking through the Apps.

However, we found that these instructions were not sufficiently explanatory to users to effectuate a mobile opt-out. This is because i) the industry-developed pages linked by Mammoth were focused on opting-out of IBA occurring through web browsers and ii) Mammoth did not provide any instructions to users on how to enable settings on their mobile devices to limit mobile IBA. Finally, we did not locate a statement of adherence to the DAA Principles during our review.

ii. Precise location data review

During our testing of the iOS version of the Wishbone app, the Accountability Program identified a third-party company collecting geolocation data in the form of GPS coordinates to the 15th decimal place. This data specified a location within thirty meters of our testing device’s location. Because we believed this data to be sufficiently accurate and precise to qualify as precise location data,¹⁴ the Accountability Program, the Accountability Program questioned whether Mammoth had any compliance obligations under the precise location data provisions of the Mobile Guidance.

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

ISSUES RAISED

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.¹⁵

¹³ Mammoth, *Mammoth Media Privacy Policy* (March 6, 2018), <https://static1.squarespace.com/static/588be02d29687fbf2f9d3cfc/t/5a9f2ebd8165f526fc525cfa/1520381629441/MammothPrivacy.pdf> [perma: <https://perma.cc/9SXZ-8ZPF>]

¹⁴ *Mobile Guidance* Definition K at 9 (“Precise Location Data is data obtained from a device about the physical location of the device that is sufficiently precise to locate a specific individual or device.”).

¹⁵ *Mobile Guidance* at 17.

i. First-party cross-app enhanced notice link 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.¹⁶ 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.¹⁷

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.¹⁸

ii. Precise location data requirements

Notice requirement

According to section IV.A.(1) of the Mobile Guidance, first parties must provide clear, meaningful, and prominent notice when they affirmatively authorize third parties to collect precise location data for use in IBA from or through their application(s).¹⁹ This notice must be placed on the company’s website or be accessible through its app(s) and provide clear descriptions of: (1) the fact that precise location data is transferred to or collected by any third party, (2) instructions for accessing and using a tool for providing or withdrawing consent, (3) **and** the fact that the first party adheres to the DAA Principles.²⁰

¹⁶ *Id.*

¹⁷ *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*, <http://www.asrcreviews.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.”).

¹⁸ DAA, *AppChoices*, <https://youradchoices.com/appchoices> (last visited Nov. 12, 2019).

¹⁹ *Mobile Guidance* at 21.

²⁰ *Id.* at 21-22.

Enhanced notice requirement

In addition to the general notice requirement under section IV.A.(1) of the Mobile Guidance, first parties must provide enhanced notice as discussed in section IV.A.(3).²¹ This enhanced notice must be a clear, meaningful, and prominent notice of the fact that the first party authorizes third-party collection of precise location data (or transfers such data to third parties). The first party must also provide a link within the enhanced notice to the disclosure required under section IV.A.(1) of the Mobile Guidance.²² This notice and link can be provided during the process of downloading the application, at the time the application is opened, **or** at the time such data is collected **and** in the application's settings or any privacy policy.²³ Companies may use the mechanisms provided by the application store to fulfill this notice requirement.²⁴ A company may also supply its own method of enhanced notice as long as it is as clear, meaningful, and prominent as the notice required by § IV.A.(3) of the Mobile Guidance.²⁵

Consent requirement

Further, under section IV.B.(1), first parties should obtain consent to allow third parties to collect precise location data for IBA purposes prior to collection.²⁶ This consent tool should be easy to use and should apply to the application and device from which the consent is provided.²⁷ The first party is also required to provide an easy-to-use tool for withdrawing consent at any time.²⁸ Under the Mobile Guidance, valid consent requires an action in response to a “clear, meaningful, and prominent notice.”²⁹ A company can satisfy this principle by allowing consumers to provide or withdraw consent as a part of the process of downloading and installing an application or through an application's settings.³⁰ A company may also use permissions tools provided by an application platform or application market provider to satisfy this requirement.³¹

COMPANY RESPONSE AND ANALYSIS

In response to the Accountability Program's inquiry letter, Mammoth 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 provided detailed descriptions of its data collection practices, worked diligently to find comprehensive solutions to

²¹ *Id.* at 23-24.

²² *Id.* § IV.A.(3)(b) at 24.

²³ *Id.* Commentary to § IV.A.(3) at 24 (“A First Party can satisfy the requirement to provide download notice under Section IV.A.3.a by participating in a notice mechanism that satisfies this Principle and is offered by an application platform or an application market provider that makes the application available for download.”).

²⁴ *Mobile Guidance* at 24-25. We note that in order to be compliant, any application store notice must meet the requirements of the Mobile Guidance, including notice of transfer to third parties.

²⁵ *Id.* at 23.

²⁶ *Id.* at 25-26.

²⁷ *Id.* § IV.B.(1)(a) at 25.

²⁸ *Id.* § IV.B.(1)(b) at 26.

²⁹ *Mobile Guidance* Definition B at 4.

³⁰ *Id.* Commentary to § IV.B.(1) at 27. The application settings may only be used by the first party to satisfy this requirement it provides notice of transfer of location data to a third party.

³¹ *Id.*

each issue, and consulted with the Accountability Program on its plan to come into compliance with the DAA Principles, as explained below.

i. Compliance with cross-app data collection requirements

Mammoth’s authorization of third-party collection of unique identifiers for IBA in its mobile apps triggered compliance responsibilities under the first-party cross-app provisions of the Mobile Guidance. Consequently, Mammoth should have provided an enhanced notice link to a compliant cross-app IBA disclosure. However, at the time of our inquiry Mammoth provided no enhanced notice link and a partially compliant disclosure.

To resolve its issues under the enhanced notice provisions of the Mobile Guidance, Mammoth took a number of steps. To start, the company elected to employ the “jump link” method of providing cross-app enhanced notice under the Mobile Guidance.

As detailed above, 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.³² In practice, a common means for providing enhanced notice before collection occurs is by placing a link on the app’s listing in an app store. However, 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.³³ To do so, app publishers must place an IBA disclosure or a link (usually a “jump link” to a later portion of the same document) to a disclosure at the top of the privacy policy linked from the app store.³⁴ 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 achieve compliance in this way, Mammoth published a new privacy policy, accessible from its website and mobile apps, that includes a jump link at the top of the document.³⁵ This jump link, labelled “Targeted Advertising,” directs users to a section of the policy that describes third-party IBA occurring through its apps.

Mammoth also agreed to modify its IBA disclosure as part of updating its privacy policy. Originally, Mammoth provided links to the Network Advertising Initiative’s (NAI) opt-out portal and DAA’s WebChoices tool, but it did not describe how users could opt-out of mobile IBA. Rather, the company stated only that consumers could “learn more about advertising networks

³² *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.

³³ *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.”).

³⁴ *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).

³⁵ Mammoth, *Privacy Policy* (Aug. 19, 2019), <https://mammoth.la/privacy>.

and interest-based advertising” by visiting these pages. And though Mammoth’s website privacy policy referenced using device-level settings to opt-out of mobile IBA, the company did not provide any instructions on accessing these settings. While the links and language provided by Mammoth were better than nothing,³⁶ they were not sufficient to comply with the Mobile Guidance.

The Accountability Program underscores that links to industry-developed opt-out pages should be accompanied by more than vague generalities. When reading Mammoth’s old IBA disclosure, a consumer might not realize that the DAA and NAI links would even lead to an opt-out tool, and certainly not that mobile-specific opt-out information may be just a few more clicks away. Despite Mammoth’s good intentions, under this implementation, only the most inquisitive consumers would have been able to opt out of IBA occurring through its mobile apps. Moreover, while Mammoth referenced device-level settings in its website privacy policy, references to these settings without additional explanatory language are unlikely to be useful to the average user. The Accountability Program has addressed this issue before in our *VRTCAL* decision, where we stated, in pertinent part:

The Accountability Program acknowledges that VRTCAL had provided users with language referring to OS-level settings as a means to opt out of its IBA and a link to the NAI’s Mobile Choices page. However, neither of these opt-out sections of VRTCAL’s privacy disclosures provided sufficiently clear instructions to render the associated opt-out mechanisms easy-to-use under the Mobile Guidance. This is because VRTCAL’s descriptions of its supported opt-out mechanisms lacked sufficient explanatory information to guide a reader to easily register their choice to opt out of IBA, rendering the mechanisms difficult to use for the typical end user. . . . references to system-level settings that are not accompanied with instructions on how to access these settings are unlikely to assist the average user in opting out of IBA.³⁷

Mammoth’s updated IBA disclosure includes a link to the DAA’s AppChoices landing page (<https://youradchoices.com/appchoices>) with additional instructions to users on downloading the AppChoices app in order to opt-out of mobile IBA. Mammoth also added a statement of adherence to the DAA Principles to its updated privacy policy.

Now, when consumers tap on the privacy policy links for the Wishbone and Yarn pages in the app stores, they will be able to immediately access information about IBA which includes a description of an easy-to-use mobile opt-out mechanism. The Accountability Program found that these actions resolved Mammoth’s compliance issues under the first-party cross-app enhanced notice provisions of the Mobile Guidance.

³⁶ *In re: Bearbit Studios*, (62-2016), May 4, 2016 at 3.

³⁷ *In re: Vrtcal Markets, Inc.* (90-2018), Dec. 10, 2018 at 7-8.

ii. Compliance with precise location data requirements

The first DAA Principles recognized the distinction between the use of standard data types for IBA versus more sensitive data like financial or medical information.³⁸ The Mobile Guidance reserved those norms of sensitivity and recognized that other, mobile-specific data types may also bear heightened scrutiny. The requirements for the collection and use of precise location data for IBA were crafted by industry in recognition of the sensitivity surrounding these particular categories of data.³⁹

Following its internal compliance review process, Mammoth informed the Accountability Program that it had disabled the third-party collection of precise location data occurring through its Wishbone app. The Accountability Program conducted subsequent testing of the company's apps, which corroborated Mammoth's claim. Noting that since there were no longer any existing IBA practices that triggered the precise location data requirements of the Mobile Guidance, the Accountability Program found that this issue was resolved.

CONCLUSION

Today's case follows a long line of cases outlining the requirements for app and website publishers to provide users with enhanced notice about third-party data collection occurring on their properties. First parties must provide a timely, up-front notice to users about this background data collection. When first parties authorize third parties to collect data through their mobile app, they must provide clear instructions to users in their disclosures on how to opt out of this collection. When companies choose to rely on industry pages or operating-system level settings to serve as their preferred methods for consumer opt-out tools, they must make sure they are taking advantage of these methods appropriately by providing clear instructions and direct links to the resources consumers need to use these tools effectively.

Here, Mammoth demonstrated its commitment to serving its customers by modifying its privacy disclosures to provide enhanced notice describing mobile data collection for IBA and a clear description of a mobile-specific opt-out tool – the DAA's AppChoices app. Mammoth's consumers will now have the benefits of transparency and choice when engaging with the company's social media and storytelling apps.

The Accountability Program recognizes the efforts that Mammoth took to achieve compliance with the Mobile Guidance and applauds the company for its commitment to industry self-regulation and user privacy. Mammoth serves as an example to other mobile app publishers.

³⁸ *OBA Principles* § VI. at 16–17.

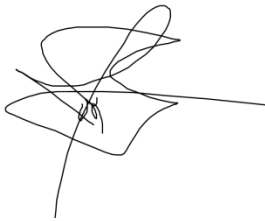
³⁹ *In re: Spinrilla (61-2016)*, May 4, 2016 (“As mobile apps are technically markedly different from websites, entities that engage in IBA through apps require specific guidance for compliance implementation that takes into account the technical issues of providing transparency and choice in the mobile world. The Mobile Guidance also takes account of apps’ and websites’ abilities to collect both precise location and user directory data, information that consumers feel is more sensitive than typical cross-site or cross-app data.”).

COMPANY'S STATEMENT

We are a strong supporter of transparency and consumer choice, and are committed to implementing and maintaining responsible online advertising practices consistent with those required under the DAA Self-Regulatory Principles. We appreciate the Accountability Program providing guidance to assist in enhancing its disclosures in its privacy policies and achieving compliance with the DAA Self-Regulatory Principles.

DISPOSITION OF DECISION

Practices voluntarily corrected.

A handwritten signature in black ink, appearing to read "Jon M. Brescia". The signature is stylized with several loops and a long horizontal stroke extending to the right.

Jon M. Brescia
Vice President
Digital Advertising Accountability Program