

BBB NATIONAL PROGRAMS

DIGITAL ADVERTISING ACCOUNTABILITY PROGRAM

COMPANY:

Azerion

CHALLENGER:

Digital Advertising Accountability Program

FORMAL REVIEW

Case Number: 122-2021

DECISION

DATE: March 9, 2021

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 publishers that authorize third parties to collect cross-app² 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). Further, when an app or a website is directed to children under the age of 13, it must also meet the requirements of the Sensitive Data Principle of the *Self-Regulatory Principles for Online Behavioral Advertising*, which requires that covered companies that collect and use “personal information” (PI) as defined in the Children’s Online Privacy Protection Act of 1998 (COPPA) for IBA do so only in compliance with COPPA.³ DAA codes of conduct are independently

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 *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.”).

³ *OBA Principles* § VI.A. at 16-17. (“Entities should not collect ‘personal information,’ as defined in the Children’s Online Privacy Protection Act (“COPPA”), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online

enforced by the Digital Advertising Accountability Program (Accountability Program), a division of BBB National Programs.⁴

COMPANY STATUS

Azerion is a website and app publisher based in the Amsterdam, Netherlands.⁵ The company owns a number of different websites and mobile apps, including the gaming website girlsgogames.com (GGG website) and the app My Dolphin Show (MDS app), available on the Android and iOS operating systems.⁶

INQUIRY

This case arises from the Accountability Program’s joint monitoring activities with the Children’s Advertising Review Unit (CARU) for apps and websites that appear primarily directed at children.⁷ The Accountability Program and CARU identified the MDS app, which prompted us to review the app for compliance with our self-regulatory principles. During the course of our inquiry, the original publisher of the MDS app and the GGG website was acquired by Azerion. The findings described in this opinion address the original privacy practices and documents of the MDS app and the GGG website, for which Azerion assumed responsibility as a result of their acquisition.⁸

I. Mobile app data collection compliance review

The Accountability Program downloaded the MDS app to our test devices. Upon downloading and launching the app, we observed data collection by third-party companies known to engage in interest-based advertising (IBA). Specifically, we noted the collection of Android’s Advertising

Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA.”)

⁴ See generally, BBB National Programs, Inc., *Digital Advertising Accountability Program*, <https://www.bbbprograms.org/programs/daap/iba-contact-us> (last visited May 26, 2020).

⁵ See generally Azerion, <https://www.azerion.com/> (last visited Oct. 5, 2020).

⁶ See Azerion, *Girls Go Games*, www.girlsgogames.com (last visited October, 2020). Apple App Store, My Dolphin Show, <https://apps.apple.com/us/app/my-dolphin-show/id632016921> (last visited Oct. 5, 2020). Google Play Store, My Dolphin Show, <https://play.google.com/store/apps/details?id=com.spilgames.mydolphinshow&hl=en&gl=US> (last visited Oct. 5, 2020). As discussed in this letter, though the apps’ pages in the app stores are listed as being published by SPIL Games, the Accountability Program understands that Azerion acquired SPIL games and all of its digital products at some point in 2019.

⁷ The Accountability Program notes that this decision only covers Azerion’s compliance with the DAA Principles. Our partners at CARU released their own decision covering compliance with the CARU guidelines, *available at* <https://case-report.bbbnp.org/Search/Index>. See also Children’s Advertising Review Unit, *Self-Regulatory Program for Children’s Advertising* (2014), <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/self-regulatory-program-for-childrens-advertising-revised-2014-.pdf>

⁸ See *OBA Principles* Definition E at 10 (“Control of an entity means that one entity (1) is under significant common ownership or operational control of the other entity, or (2) has the power to exercise a controlling influence over the management or policies of the other entity.”)

ID (AAID or IFA) and Apple’s Identifier for Advertising (IDFA).⁹ The collection of this data prompted us to review the app for compliance with the Mobile Guidance’s first-party provisions and the Sensitive Data Principle of the OBA Principles.

i. Mobile enhanced notice requirement

While testing My Dolphin Show, the Accountability Program was unable to find an enhanced notice link in any of the times or locations prescribed by the Mobile Guidance. While the App provided links to the company’s privacy policy for mobile apps within its listings on the Google Play Store and the Apple App Store, these links do not take users directly to a section of the privacy policy that discloses the third-party IBA activity SPIL allows through its App.¹⁰ Looking further, the Accountability Program examined the mobile app privacy policy to determine if the company offered any elements of a compliant disclosure of third-party IBA activity taking place through its apps. While we located language describing that app publisher may authorize third parties to collect data through its mobile apps for IBA, we were unable to locate a mobile opt-out mechanism, a core requirement of section III.A.(3) of the Mobile Guidance. Finally, we could not find a statement of adherence to the DAA Principles.

ii. Sensitive Data Principle

During its review, we noted that the MDS app included elements that lead the us to believe it is directed to children.¹¹ In particular, the app is an easy animated game where a user directs the movements of a dolphin in a water park. Further, the app’s pages in the app stores state, in pertinent part, that the game is “[s]afe fun for kids of all ages” and “[t]his game, for girls and boys of all ages, is free to play.” We also noted that the app publisher stated in its dedicated mobile app privacy policy that the app publisher “does not knowingly process personal data from anyone under the age of 16 without parental consent.”

Nonetheless, the Accountability Program found through network traffic analyses that third parties were collecting the unique device-specific advertising identifiers from our test devices through our use of the MDS app. Some of these third parties are known to the Accountability Program to engage in IBA as part of their routine business activities. We further noted that the app did not obtain verifiable parental consent prior to collection, nor did it employ an age gate to screen users under the age of 13, as required under COPPA. Assuming that the MDS app was directed to children under the age of 13, we found that these actions appeared to be inconsistent with the Sensitive Data requirements of the DAA Principles and COPPA.

⁹ 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.”).

¹⁰ SPIL, *Mobile Privacy Policy – EN* (May 25, 2018), <https://spilgames.com/mobile-apps-privacy-policy/>.

¹¹ For further reading on the relevant elements in this analysis, see Complaint For Civil Penalties, Permanent Injunction, and Other Equitable Relief, *United States v. TinyCo*, 3:14-cv-04164 (N.D. Calif. Sept. 16, 2014), <https://www.ftc.gov/system/files/documents/cases/140916tinycocmpt.pdf>.

II. Website data collection compliance review

The Accountability Program and CARU went on to examine a website that was owned by the same publisher as My Dolphin Show, located at www.girlsgames.com. There, we identified third parties collecting data on the website, likely for IBA. We went on to examine this website for compliance with the Sensitive Data provisions of the OBA Principles.¹²

The Accountability Program noted that the GGG website included elements that lead us to believe it is a child-directed site, such as games featuring young characters in costume engaging in play and dress up. We further noted that the website's "Parents Information" disclosure stated, in pertinent part, that:

GGG.com is an online games site for young girls with a large variety of dress-up games, design games, cooking games, and other fun games. Through these games, girls learn to play interactively with their peers. And since we add new games every day, girls won't get bored easily!¹³

The Accountability Program found that the elements of the games featured on the GGG website and the language in the Parents Information disclosure suggested that the website was directed to children. Consequently, we also reviewed the application for compliance with the portion of the Sensitive Data Principle related to children, section VI.A. of the OBA Principles. This section requires that all companies which are covered by the DAA Principles may only collect persistent identifiers from children they know to be under the age of 13 or from child-directed sites in compliance with COPPA. Despite this, we observed third parties collecting data for IBA during our web browsing session, observing further that the website did not obtain verifiable parental consent prior to collection, nor did it employ an age gate to screen users under the age of 13, as required under COPPA. Assuming that the GGG was a child-directed website, we found that it did not appear to comply with the Sensitive Data Principle of the OBA Principles.

Acting on this analysis, the Accountability Program and CARU subsequently reached out to the website and app publisher with an inquiry letter, explaining the requirements of their self-regulatory programs, explaining the review process, and requesting the company's responses to our compliance questions.¹⁴

¹² The Accountability Program notes we identified ads with the DAA's AdChoices Icon, which may serve as enhanced notice for websites under the DAA Principles. We note that the presence of this icon does not negate any issues a website has under any other compliance issue under the Principles, including compliance with the Sensitive Data provision.

¹³ SPIL, *Parents Information*, <http://www.girlsgames.com/parents-information> (last visited May 9, 2019). The Accountability Program notes that website www.girlsgames.com appears to host a number of games that may be child directed. The Accountability Program also notes that SPIL states in its *Mobile Apps Privacy Policy Kids and Parents* that SPIL "[does] not permit behaviorally-targeted advertising to children in our mobile games where we have actual knowledge that the user is under the age of 13." The Accountability Program notes that this language appears to be in tension with the data collection that we observed occurring through the App, and that we did not observe any type of age-gate mechanism during our testing of the App. SPIL, *Mobile Apps Privacy Policy Kids and Parents* (Jan. 9, 2017), <https://spilgames.com/parents/>.

ISSUES RAISED

I. 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 cross-app data through their apps for use in IBA, they must provide enhanced notice and choice about such third-party data collection for IBA.¹⁵

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

II. Sensitive Data Principle of the OBA Principles

As we have discussed at length in prior relevant decisions,¹⁸ the OBA Principles' Sensitive Data Principles triggers heightened responsibilities when companies authorize the collection of certain types of data, including the persistent identifiers that underpin IBA, through applications or websites that are directed to children.¹⁹ Compliance with the Sensitive Data Principle requires,

¹⁵ *Mobile Guidance* at 17.

¹⁶ *Id.* See generally *In re FitNow, Inc.* (101-2019), Sep. 5, 2020, *In re: Publishers Clearing House, Inc.* (92-2019), Jan. 28, 2019), *In re: Finish Line*, (86-2018), Sep. 26, 2018).

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. See also Accountability Program, *Compliance Warning*, https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/accountability-program/v.-accountability-program-guidance/accountability-program-first-party-enhanced-notice-compliance-warning-cw-01-2013.pdf?sfvrsn=25e3af96_2at 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 See, e.g., *In re: Top Free Games*, Accountability Program Decision 63-2016 (May 4, 2016), <https://www.bbb.org/globalassets/local-bbbs/council-113/media/behavioral-advertising/top-free-games-decision.pdf>.

¹⁹ *Mobile Guidance* at 1.

among other things, compliance with the pertinent provisions of COPPA.²⁰ COPPA, in part, requires companies to obtain verifiable parental consent²¹ when they 1) allow the collection of PI²² from children they have actual knowledge are under the age of 13, or 2) allow the collection of PI on applications that are directed to children.²³ Since our testing revealed third-party collection of persistent identifiers (a type of PI under COPPA) through the MDS app and GGG website, which appeared likely to attract a significant audience under 13, we determined that GGG had heightened responsibilities under the Mobile Guidance. In analyzing these responsibilities, we examined the FTC’s body of COPPA cases.

Under section 312.2 of the FTC’s COPPA regulations, the determination of whether an application is targeted to children is based on a multi-factor test which considers factors such as subject matter, visual content, language, use of animated characters, and use of child-oriented activities or incentives.²⁴ The FTC recently addressed this issue in its *HyperBeard* settlement.²⁵ In that case, the FTC alleged that the company’s mobile apps were child-directed because they “contain[ed] brightly colored, animated characters including cats, dogs, bunnies, chicks, monkeys and other cartoon characters.” In addition, the apps had “subject matters . . . highly appealing to children,” including, e.g., “collecting smiley cats, dogs, chicks, eggs, coins and gems, as well as baking with animated bunnies” and were “very simple and easy to play.”²⁶

In its official FAQs for COPPA, the FTC strongly encourages a company to investigate whether its app falls within the FTC definition of “child-directed” (that is, whether it has either a primary or secondary audience of children under 13).²⁷ Further, COPPA imposes strict liability on the

²⁰ *OBA Principles* at 16-17. *See also* Children’s Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6505.

²¹ 15 U.S.C. § 6501(9).

²² Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, § A.3., <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> (last visited Apr. 6, 2016). (“The amended Rule defines personal information to include . . . A persistent identifier that can be used to recognize a user over time and across different websites or online services.”) *See also* 15 U.S.C § 6501(8).

²³ *Id.*, *see also supra* note 17.

²⁴ *See supra* note 19 at § D.1. (“The amended Rule sets out a number of factors for determining whether a website or online service is directed to children. These include subject matter of the site or service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, or whether advertising promoting or appearing on the website or online service is directed to children.”)

²⁵ *See generally* *FTC v. HyperBeard, Inc.*, FTC Matter 192 3109 (June 2020); *see also* *FTC v. TinyCo*, FTC Matter 132 3209 (Sept. 2014).

²⁶ Complaint at 9–10, *United States v. HyperBeard, Inc.*, No. 3:20-cv-3683 (N.D. Cal. June 3, 2020).

²⁷ *See supra* note 19 at § D.3. (“As the operator, you should carefully analyze who your intended audience is, the actual audience, and in many instances, the likely audience for your site or service.”) *See also supra* note 19 at § G.2. (“Although you may intend to operate a “teen service,” in reality, your site may attract a substantial number of children under 13, and thus may be considered to be a “Web site or online service directed to children” under the Rule. Just as the Commission considers several factors in determining whether a site or service is directed to

owners and operators of child-directed websites and online services where third parties collect PI from children for IBA.²⁸ This precludes first parties from disclaiming data collection practices in their privacy policies with respect to children under the age of 13 if the FTC deems the app to be child-directed based on the multi-factor test the agency has developed or from disclaiming responsibility for the actions of third parties on its app or website.

COPPA allows the designation of some child-directed apps as “mixed-audience” when the app does not target children as its primary audience but nonetheless “attract[s] a substantial number of children under 13.”²⁹ COPPA allows publishers to employ an age screen in these circumstances to flag users under the age of 13 so first parties can prevent third parties from collecting their data, obtain verifiable parental consent prior to collection, or direct the children to content that does not involve the collection or use of PI.³⁰

COMPANY RESPONSE AND ANALYSIS

After Azerion had acquired the GGG website and MDS app, the company made contact with the Accountability Program and CARU and clarified its ownership of those properties. The company quickly committed to compliance with the DAA Principles, and worked with the Accountability Program to take several actions to ensure that its website and app met the requirements of the DAA Principles, described below.

I. Mobile data collection issues for IBA

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

children, you too should consider your service’s subject matter, visual content, character choices, music, and language, among other things. If your service targets children as one of its audiences – even if children are not the primary audience – then your service is “directed to children.” In circumstances where children are not the primary audience of your child-directed service, the amended Rule allows you to employ an age screen in order to provide COPPA’s protections to only those visitors who indicate they are under age 13. Note that sites or services directed to children cannot use the age screen to block children under age 13.”)

²⁸ Children’s Online Privacy Protection Act Rule; Final Rule, Vol. 38 No. 12, 16 C.F.R. Part 312 (2013), <http://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf>. (“For the reasons discussed below, the Commission, with some modifications to the proposed Rule language, will retain the strict liability standard for child-directed content providers that allow other online services to collect personal information through their sites.”) *See also*, 15 U.S.C. § 6501(2). (“The term “operator”— (A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce....”)

²⁹ *See supra* note 25.

³⁰ *Id.*

disclosure.³¹ 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.³² 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.³³ 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.

II. Sensitive Data provision

During its discussions with Azerion, the Accountability Program impressed upon the company the need to account for all third-party data collection occurring through its online services to ensure it was meeting its obligations under COPPA and the sensitive data provision. Working with the Accountability Program and CARU, Azerion took several steps to reach compliance with these requirements.

i. MDS app

Azerion conducted an audit of third-party data collection occurring on its app and found that the device advertising identifier was being collected by the app’s servers, as well as third-party advertising partners, even under certain circumstances when the app’s “age gate” had been set to indicate that the app user was under 13 years old. To ensure compliance with the Sensitive Data provision, Azerion removed advertising entirely from the MDS app and engaged an outside auditor to review its changes. After testing this new version of the MDS app, the Accountability Program found that it was no longer transmitting PI, either to the app servers or to third parties, bringing the MDS app into compliance with the Sensitive Data Principle.

ii. GGG website

After consulting with the Accountability Program, Azerion disabled all third-party data collection for IBA on the GGG website, disabling all data-sharing and remarketing with their third-party advertising partners. Azerion also engaged an outside auditor to review advertising

³¹ *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.

³² *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.”).

³³ *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). See also *In re: Mammoth Media, Inc. (112-2020)*, Apr. 3 2020 at 7.

practices on the website, who verified that no third-party tracking of individuals was taking place after the changes. Additionally, Azerion updated its internal guidelines and practices to ensure ongoing compliance. Finding that there were no longer any existing practices that were out of compliance with the Sensitive Data Provision, the Accountability Program found that this issue was resolved.

CONCLUSION

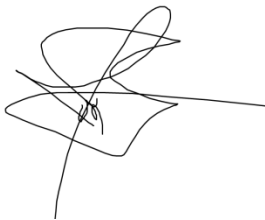
Today's case again highlights the need for companies who make kids' websites or apps to pay special attention to the kinds of data they collect—or allow to be collected. Given the widely acknowledged sensitivity of children's data, reviews of such companies' ad partnerships (whether in the form of banner ads on a website or SDKs bundled with mobile apps) are essential. We are pleased that Azerion immediately recognized the seriousness of the issues at hand and committed to full compliance with the DAA Principles.

COMPANY'S STATEMENT

We appreciate CARU's comprehensive evaluation and guidance for the Website and App. After the acquisition of these products, it has been our pleasure to work with CARU towards identifying the areas for improvement and industry best practices for child appropriate design. During this process, we also had the opportunity to follow more closely and participate in CARU's trainings and seminars. We have taken the recommended steps in the Website and App. Our business value relies fully on providing a safe and reliable entertainment ecosystem, and thus, we will continuously maintain and improve the compliance of our products.

DISPOSITION OF DECISION

Practices voluntarily corrected.

A handwritten signature in black ink, appearing to read 'Jon M. Brescia', with a long horizontal line extending to the right.

Jon M. Brescia
Vice President
Digital Advertising Accountability Program