

BBB NATIONAL PROGRAMS, INC.

DIGITAL ADVERTISING ACCOUNTABILITY PROGRAM

COMPANY:

Appriss Inc.

CHALLENGER:

Digital Advertising Accountability Program

FORMAL REVIEW

Case Number: 123-2021

DECISION

DATE: April 7, 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 publishers² that authorize third parties³ to collect data through their apps for use in cross-app⁴ 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>.

²The 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. 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. *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.”). *See also* Accountability Program, *First Party Enhanced Notice Compliance Warning*, CW-01-2013, <https://www.bbb.org/us/Storage/113/Documents/First-Party-Compliance-Warning-20131008.pdf>.

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 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.”).

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

Appriss Inc. (Appriss) is a company that publishes the public safety app MobilePatrol, available on the Android and iOS operating systems.⁶ The company is headquartered in Louisville, Kentucky. The app has approximately 5 million downloads in the Google Play Store.

INQUIRY

This case arises from the Accountability Program's regular monitoring of mobile applications. The Accountability Program identified MobilePatrol and began reviewing it for compliance with the Mobile Guidance. As part of this review, the Accountability Program installed the iOS and Android versions of the app on our test devices and was able to capture and inspect data packets transmitted from the application. Through analysis of network traffic generated from the app, 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.⁷

i. Cross-app enhanced notice review

To assess Appriss's compliance with the mobile enhanced notice requirement, the Accountability Program first examined privacy policy links in MobilePatrol's listings in the Google Play and Apple App Stores. These links directed us to the top of a privacy policy document⁸ for Appriss. However, these links did not function as enhanced notice links, as they did not lead directly to a compliant disclosure of third-party IBA taking place through MobilePatrol. Looking further, we could not find links to a compliant IBA disclosure either during download or upon first opening the app, which are the alternative times at which enhanced notice may be provided. Likewise, we did not observe an enhanced notice link in either the privacy policy or the app settings.⁹

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 Apple App Store, *MobilePatrol: Public Safety*, <https://apps.apple.com/us/app/mobilepatrol-public-safety/id620067490> (last visited Jan. 12, 2020). Google Play Store, *MobilePatrol Public Safety App*, https://play.google.com/store/apps/details?id=com.appriss.mobilepatrol&hl=en_US&gl=US (last visited Jan. 12, 2020).

⁷ 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.").

⁸ Appriss, *Privacy Policy* (July 31, 2019), <https://appriss.com/privacy-policy/>.

⁹ While the Accountability Program observed one third-party in-app ad with an enhanced notice link, that link did not compensate for the lack of first-party enhanced notice. Most ads lacked this third-party enhanced notice, and much of the apparent third-party data collection appeared to take place without visible ads. Thus, an enhanced notice link did not appear during most apparent third-party cross-app collection for IBA.

The Accountability Program moved on to determine if Appriss had provided any disclosure of third-party data collection for IBA taking place through its mobile app. In the Appriss privacy policy, we were unable to locate a complete IBA disclosure for third-party cross-app data collection and use through MobilePatrol. While the Appriss privacy policy,¹⁰ to which the app links, stated that Appriss may use personal data to “Deliver[] . . . targeted advertisements, promotional messages, notices and other information related to Appriss Services and your interests,” it neither described *third-party* IBA nor included a description of a mobile opt-out mechanism. Identifying a document labelled “Cookie Notice,”¹¹ the Accountability Program also found that while this document discussed tracking facilitated on smartphones by unique identifiers, it did not explicitly state that third parties may collect this data for IBA, nor did it provide a description of a mobile opt-out tool. The Accountability Program also could not locate a statement of adherence to the DAA Principles during our review.

ii. Precise location data collection review

During our testing of the Android version of Mobile Patrol, we identified a third party collecting longitude and latitude coordinates to the sixth and seventh place, which represented a degree of precision within 20 meters of our test device’s location. Believing the observed collection to be both sufficiently precise and accurate to qualify as precise location data, we moved on to review the app for compliance with the precise location data provisions of the Mobile Guidance.

Notice review

During our review, we were unable to find a complete third-party IBA disclosure for the collection of precise location data.¹² While a standard location permissions tool in the Android version of the app notified users about location data collection, the dialog did not mention the precision of this data, describe third-party use of precise location data for IBA, or contain a consent withdrawal mechanism.¹³ As noted in the [cross-app section], above, we also did not find a statement of adherence to the DAA Principles.

Enhanced notice review

¹⁰ Appriss, *Privacy Policy* (July 31, 2019), <https://appriss.com/privacy-policy/>.

¹¹ Appriss, Appriss Cookie Notice, <https://appriss.com/cookie-notice/>. (“When you visit a website, the site may collect and store information on your browser, usually in the form of cookies. A cookie is a small amount of data with a unique identifier that is sent to the web browser on your computer, tablet, or smart phone (your ‘device’) from a website’s computer and is stored on your device’s hard drive....Cookies also collect details of your behavioral patterns upon visiting our website pages. This cookie information is most often used to collect statistics about our visitors, to make the website run smoothly for your convenience, and to deliver targeted content. Information used in cookies does not usually directly identify you, but cookies can track your individual preferences in order to give you a more personalized web experience and provide information to the website operator about the site.”).

¹² The Accountability Program observed that the privacy policy stated that “We may also collect Personal Data about you from certain affiliates and other third parties, including but not limited to...Service providers that help us determine a location in order to customize certain products to your location.” We note that this does not constitute a clear disclosure that third parties may collect precise location data for IBA purposes.

¹³ Appriss, MobilePatrol, Location permission pop-up (Asking: “Allow MobilePatrol to access this device’s location?”).

We did not observe a first-party enhanced notice pertaining to third-party precise location collection at any stage during our download and use of MobilePatrol. As discussed above, while we observed a permissions tool asking for our consent to allow MobilePatrol to access our location, this permissions tool lacked information about third-party use of precise location for IBA, information about the precision of the location data, and a link to a disclosure that would have enabled users to opt out of precise location data collection after consenting to it.

User consent review

As discussed above, while testing the Android version of the Mobile Patrol app, we observed a permissions tool that requested access to the user's device's location. However, this permissions tool did not state that third parties may collect the user's precise location data for IBA purposes. We could find no other mechanism requesting user consent for this type of collection.

Following our review, the Accountability Program sent an inquiry letter to Appriss 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.¹⁴

i. 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

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*, <http://www.asrreviews.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.”).

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.¹⁷

ii. Precise location data

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).¹⁸ 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.¹⁹

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).²⁰ 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.²¹ 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.²² Companies may use the mechanisms provided by the application store to fulfill this notice requirement.²³ 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.²⁴

¹⁷ Digital Advertising Alliance, *Download the AppChoices Tool - Now with 'Do Not Sell' Enhancements*, <https://youradchoices.com/appchoices> (last visited Jan. 12, 2020).

¹⁸ *Mobile Guidance* at 21.

¹⁹ *Id.* at 21-22.

²⁰ *Id.* at 23-24.

²¹ *Id.* § IV.A.(3)(b) at 24.

²² *Id.* See *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.")

²³ *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.

²⁴ *Id.* at 23.

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.²⁵ This consent tool should be easy to use and should apply to the application and device from which the consent is provided.²⁶ The first party is also required to provide an easy-to-use tool for withdrawing consent at any time.²⁷ Under the Mobile Guidance, valid consent requires an action in response to a “clear, meaningful, and prominent notice.”²⁸ 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.²⁹ A company may also use permissions tools provided by an application platform or application market provider to satisfy this requirement.³⁰

COMPANY RESPONSE AND ANALYSIS

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

i. Compliance with cross-app data collection requirements

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

The cross-app provisions of the Mobile Guidance prescribe particular times and locations where consumers can receive enhanced notice that directs them to a compliant IBA disclosure.³¹ The link should appear either before or concurrent with the initial collection of data for IBA.³² 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

²⁵ *Id.* at 25-26.

²⁶ *Id.* § IV.B.(1)(a) at 25.

²⁷ *Id.* § IV.B.(1)(b) at 26.

²⁸ *Mobile Guidance* Definition B at 4.

²⁹ *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.

³⁰ *Id.*

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.* § III.A.(3) at 17.

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 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 resolve its issues under the enhanced notice provisions of the Mobile Guidance, Appriss took a number of steps. The company first updated its privacy disclosures to add a jump link to the top of its privacy policy labelled “AdChoices.”³⁵ This jump link directs users to an updated section of the Appriss privacy policy that describes third-party IBA occurring through the MobilePatrol app.³⁶ This new disclosure also points users to a link to the DAA’s AppChoices app and also instructs users they may opt out by accessing an Ad Choices setting integrated into the MobilePatrol app. Finally, Appriss included a statement of adherence to the DAA Principles in this disclosure. The Accountability Program found that these actions resolved Appriss’s compliance issues under the first-party cross-app enhanced notice provisions of the Mobile Guidance.

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.³⁷ The Mobile Guidance retained 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.³⁸

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 Appriss, *Appriss Privacy Policy*, <https://appriss.com/privacy-policy/#adchoices> (last visited Jan. 12, 2020). The Accountability Program additionally notes that the privacy policy link in the Google Play Store listing for MobilePatrol serves as a jump link to Appriss’s updated IBA disclosure, which is also a compliant means of providing mobile cross-app enhanced notice.

³⁶ *Id.* (“You can find more information about IBA or opt out of IBA on this browser by companies that participate in the Digital Advertising Alliance’s WebChoices tool by visiting aboutads.info/choices or opt out of IBA on mobile devices by visiting: <https://youradchoices.com/appchoices/>. Your device may also include a feature that allows you to opt out of the use of information about your use of mobile applications for IBA purposes, such as ‘Limit Ad Tracking’ for iOS devices. Also, within our Mobile Patrol app you can select ‘Ad Choices’ from the settings menu to set your choice for that app. We adhere to the Digital Advertising Alliance’s Self-Regulatory Principles.”).

³⁷ *OBA Principles* § VI. at 16–17.

³⁸ *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.”).

Following its internal compliance review process, Appriss determined that the detected third-party location data collection appeared to be unintentional and disabled such collection entirely. The Accountability Program conducted subsequent testing of the MobilePatrol app which confirmed that no third-party location data collection was taking place. 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 and provide the appropriate opt-out mechanisms. When precise location data is collected by third parties for IBA, first parties must comply with the requirements for notice, enhanced notice, and consent.

Here, Appriss demonstrated its commitment to serving its customers by modifying its privacy disclosures to provide enhanced notice describing mobile data collection for IBA and a mobile-specific opt-out tool. The company also ensured that no third-party collection of precise location data could take place. Now, consumers will now have the benefits of transparency and choice when engaging with the company's public safety app.

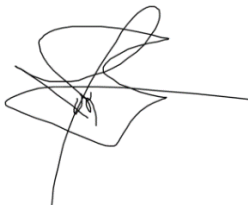
The Accountability Program recognizes the efforts that Appriss took to achieve compliance with the Mobile Guidance and applauds the company for its commitment to industry self-regulation and user privacy.

COMPANY'S STATEMENT

Appriss is committed to responsible online advertising practices within its mobile applications, and strongly supports the OBA principles of transparency and choice. We thank the Accountability Program for bringing this matter to our attention and working with us to bring our MobilePatrol public safety application into compliance with the DAA Principles.

DISPOSITION OF DECISION

Practices voluntarily corrected.

A handwritten signature in black ink, appearing to read 'Jon M. Brescia', written over a faint, stylized graphic element that resembles a signature or a logo.

Jon M. Brescia
Vice President
Digital Advertising Accountability Program