

BBB NATIONAL PROGRAMS, INC.

DIGITAL ADVERTISING ACCOUNTABILITY PROGRAM

FORMAL REVIEW

Case Number: 104-2019

)
<u>COMPANY:</u>)
WiFi Map LLC)
)
<u>CHALLENGER:</u>)
Digital Advertising)
Accountability Program)
)
)

DECISION

DATE: October 24, 2019

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 cross-app⁴ data through their

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 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 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.”).

apps for use in IBA must provide users with notice and enhanced notice, as described in the Mobile Guidance. Before allowing third parties to collect precise location data⁵ for IBA, mobile app publishers must also provide users with the opportunity to consent to this collection, in addition to enhanced notice and the standard notice of this fact.

COMPANY STATUS

WiFi Map LLC (WiFi Map) is an app publisher with a United States headquarters in New York, New York.⁶ The company offers an eponymous mobile app⁷ to the public (WiFi Map app) that crowdsources data about WiFi hotspots. According to the Google Play Store, the app has been downloaded approximately 50 million times.

INQUIRY

This inquiry arises from the Accountability Program’s continuing monitoring and enforcement efforts in the mobile app space.⁸ As part of these efforts, the Accountability Program examined the WiFi Map app on the Android and iOS operating systems for compliance with all applicable provisions of the DAA Principles. Below, we describe our review in detail.

i. Cross-app data collection review

As part of our investigation, the Accountability Program downloaded and installed the WiFi Map app on our Android and iOS test devices. Using our testing equipment, we were able to capture and inspect data packets being transmitted from the application. Through analysis of network traffic generated from the app, we observed third parties⁹ collecting cross-app¹⁰ data likely for IBA. Specifically, we noted the collection of Android’s Advertising ID (AAID or IFA).¹¹

The Accountability Program navigated to the WiFi Map app’s pages in the Apple App and Google Play Stores to examine the app’s compliance with the first-party enhanced notice provision of the Mobile Guidance. While the WiFi Map app provided privacy policy links within

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 WiFi Map, #1 WiFi Finder, <https://www.wifimap.io/> (last visited July 22, 2019).

⁷ WiFi Map, WiFi Map – Free Passwords & Hotspots, https://play.google.com/store/apps/details?id=io.wifimap.wifimap&referrer=utm_source%3Dwebsite (last visited July 22, 2019). WiFi Map, *WiFi Map: Get WiFi, VPN, Proxy*, <https://itunes.apple.com/app/apple-store/id548925969?mt=8> (last visited July 22, 2019).

⁸ For more information on the Accountability Program, and to read prior decisions referenced herein, please visit <http://www.asrcreviews.org/accountability-program-decisions/>.

⁹ *Id.* at 12 (“An entity is a Third Party to the extent that it collects Cross-App Data or Precise Location Data from or through a non-Affiliate’s application or collects Personal Directory Data from a device.”).

¹⁰ *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.”).

¹¹ 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.”).

its listings in the app stores that directed users to the top of a privacy policy document,¹² these links did not function as enhanced notice links. This is because they did not take users directly to a disclosure that describes the third-party IBA activity WiFi Map allows through its app.¹³

Looking further, we observed a full-screen “Terms of Use” dialog appear following launch of the app. It stated that “some personally identifiable information may be collected by third party SDKs” and that users can “disable data collection at any time in settings.” This dialog also contained links directing users to the top of WiFi Map’s terms of use and privacy policy documents. However, this dialog was not sufficient for providing enhanced notice as it did not specify that third parties may collect data for IBA purposes nor provide links directly to a disclosure of third-party IBA activity. We could find no other link that would serve as enhanced notice under the Mobile Guidance.

The Accountability Program looked further to determine whether WiFi Map had provided any disclosure of third-party data collection for IBA taking place through its mobile app. We found that WiFi Map’s privacy policy contained a disclosure of the fact that third parties may collect data through the application for IBA purposes.¹⁴ The policy also stated, in pertinent part: “[t]o opt out of our use of the personal information that we collect about you for advertising purposes, please contact us at support@wifimap.io with a request that we not use your personal information for advertising purposes, and we will honor that request.”

It appeared overly cumbersome to the Accountability Program that users must open an email program or app and draft correspondence to contact WiFi Map to request an opt-out. Therefore, we found that this means of opting out presented a compliance issue under the first-party enhanced notice provisions of the Mobile Guidance.

Finally, the Accountability Program could not locate a statement of adherence to the DAA Principles during its review.

ii. Precise location data collection review

During our testing of the Android version of the WiFi Map app, the Accountability Program observed a third-party company that appeared to be engaged in IBA collecting location information through the app. The location information was in the form of latitude and longitude coordinates to the sixth decimal place.

During our review of WiFi Map’s privacy disclosures, the Accountability Program found language indicating that precise location data may be transferred to third parties for IBA

¹² WiFi Map, *WiFi Map – Privacy Policy* (May 23, 2018), <https://www.wifimap.io/privacy> [perma: <https://perma.cc/Y5MV-W4S3>].

¹³ *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).

¹⁴ WiFi Map, *WiFi Map – Privacy Policy* (May 23, 2018), <https://www.wifimap.io/privacy> [perma: <https://perma.cc/Y5MV-W4S3>].

purposes. However, we found neither a tool for providing or withdrawing consent¹⁵ regarding the collection of precise location data nor a statement of adherence to the DAA Principles.

Furthermore, the Accountability Program was unable to locate any enhanced notice disclosure or link that informed users about the collection of precise location data for IBA in any of the times and locations prescribed by the Mobile Guidance. As discussed above in our cross-app data review, we noted that we observed a “Terms of Use” dialog appear following launch of the app. However, this dialog was not sufficient for providing enhanced notice, as it neither specified that third parties may collect precise location data from users for IBA purposes, nor directed users to a disclosure describing how to withdraw consent for this collection.

Finally, after launching the WiFi Map app the Accountability Program observed an additional dialog box requesting that users enable location for the purpose of “display[ing] all nearby WiFi Hotspots.” This dialog was paired with a system-default permissions tool that requested consent before allowing the collection of location data from the device. However, the dialog and permissions tool did not include any language disclosing that third parties received precise location data through the WiFi Map app for IBA purposes. Looking further, we could not locate any disclosure that would make clear to users that this consent mechanism would result in the third-party collection of their precise location data for IBA, raising a compliance issue under this provision of the Mobile Guidance.

Following our review, the Accountability Program sent an inquiry letter to WiFi Map 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.¹⁶

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.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

¹⁵ The Accountability Program notes that the privacy policy generally referenced the permissions tools that the major operating systems utilize to obtain consent for the use of location data. However, we did not locate any additional instructions or mechanisms for users to withdraw consent for the collection of precise location data on the app level. WiFi Map, *WiFi Map – Privacy Policy* (May 23, 2018), <https://www.wifimap.io/privacy> [perma: <https://perma.cc/Y5MV-W4S3>].

¹⁶ *Mobile Guidance* at 17.

¹⁷ *Id.*

of the app, **or** at the time cross-app data is first collected, **and** in the application’s settings or any privacy policy.¹⁸

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 replaces the old-fashioned practice of burying information about IBA—if it was provided at all—somewhere in the privacy policy for the consumer to unearth. 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.

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).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

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

¹⁸ *Id.*

¹⁹ *Mobile Guidance* at 21.

²⁰ *Id.* at 21-22.

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.

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

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* § I.B. at 4.

³⁰ *Id.* Commentary to § IV.B.(1) at 27.

³¹ *Id.*

COMPANY RESPONSE AND ANALYSIS

In response to the Accountability Program’s inquiry letter, WiFi Map immediately conducted a thorough review of its compliance with the DAA Principles. The company 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

WiFi Map’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 Mobile Guidance prescribes particular times and locations where consumers can receive enhanced notice that directs them to a compliant IBA disclosure.³² The link should appear either before or concurrent with the initial collection of data for IBA.³³ One means for providing enhanced notice before collection occurs is by providing it 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.³⁴ 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.

Critically, the Mobile Guidance also requires that enhanced notice points to a choice mechanism that either meets DAA specifications or individually lists each third party collecting IBA, to ensure ease of use by a consumer. In prior casework,³⁵ we have noted that mobile opt-out mechanisms do not meet industry standards for ease of use when users must draft an email or prepare postal mail to a company to request an opt out.

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 *Mobile Guidance* § III.A.(3) at 17.

³⁴ *Mobile Guidance* Commentary 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.”).

³⁵ *See In re: IQM Corporation (96-2019)*, May 22, 2019 at 12 (“Similarly, in this case we raised concerns with IQM about the company’s mobile opt-out mechanism, which required users to obtain their device identifiers by utilizing a third party mobile app or access the identifier through their device’s settings, and then write an email containing this identifier to IQM requesting that the user be opted out of IQM’s IBA.”) *See also In re: LKQD Technologies, Inc. (77-2017)*, December 11, 2017 at 3-4. (“The Accountability Program questioned whether requiring a user to draft and mail a physical letter to the company’s corporate headquarters in order to exercise choice with respect to IBA was overly burdensome to consumers and too protracted a process.”).

During discussions with WiFi Map, the Accountability Program emphasized that an opt-out tool that requires a user to open an email app or program and provide the necessary details about their device or household does not meet the requirements in the Mobile Guidance that a choice mechanism for IBA be easy to use. We also noted that a privacy-sensitive user might be uncomfortable engaging in these tasks, which require her to reach out to the company and provide additional details about her device, such as her IDFA/IFA/AAID, IMEI/MEID, UDID, MAC address, etc, and perhaps her personal identity, which is often tied inextricably to the person's email address. Therefore, we found that WiFi Map's opt-out mechanism did not meet the requirements under the Mobile Guidance.

WiFi Map acknowledged our findings and swiftly took a number of actions to meet the relevant compliance requirements. The company modified the IBA disclosure of its privacy policy to include links to instructions on accessing device-level settings to opt out of mobile cross-app IBA. The company also added to this disclosure a statement of adherence to the DAA Principles. To provide enhanced notice to users, WiFi Map added a jump link to the top of its privacy policy, labeled "Interest Based Ad Disclosure," directing users to this IBA disclosure.

WiFi map also updated its terms of use dialog that appears in the Android version of its app to add language indicating that third parties may collect data from users for IBA. The company also updated this dialog to include a link that takes users directly to its IBA disclosure, described above.

As a result of the company's updates, described above, a mobile app user is now able reach important information about IBA occurring through the WiFi Map app by simply tapping on either the privacy policy links in the app stores or the link in the Android app's terms of use dialog. Additionally, WiFi Map's IBA disclosure now includes methods for users to easily exercise choice about IBA occurring through mobile devices. The Accountability Program found that these steps resolved WiFi Map's first-party cross-app issues under the Mobile Guidance.

ii. Compliance with precise location data requirements

The OBA Principles recognized the distinction between standard data types for IBA versus more sensitive data like financial or medical information.³⁶ The Mobile Guidance reserved those notions of sensitivity and recognized that other, mobile-specific data types may also bear heightened scrutiny. Consequently, the Mobile Guidance requires consumers to provide consent when first parties authorize the third-party collection of precise location data for IBA purposes. This consent is in addition to the standard notice and enhanced notice that must be given to consumers regarding precise location information. These requirements were crafted by industry in recognition of the sensitivity surrounding this category of data.³⁷

³⁶ *OBA Principles* §VI.at 16-17.

³⁷ *In re: Spinrilla (61-2016)*, May 4, 2016, <https://www.bbb.org/globalassets/local-bbbs/council113/media/behavioral-advertising/spinrilla-decision.pdf> ("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.").

The authorization of the third-party collection of location data sufficient to identify a particular user or device for IBA purposes in the Android version of its app triggered WiFi Map's obligations to provide notice and enhanced notice to users about this collection and to get their consent prior to allowing it. During discussions with the company, the Accountability Program emphasized that standard permissions tools or dialogs that only refer to the collection of precise location data for the app's functionality are not sufficient to meet the requirements of the Mobile Guidance, as consumers must receive enhanced notice and the ability to consent to the third-party collection of this type of sensitive data.

Acknowledging our findings and the imperatives of the Mobile Guidance, the company worked with the Accountability Program to take the following actions to come into compliance with the precise location data provisions.

Notice requirement

WiFi Map updated its privacy policy to provide a clearer disclosure that third parties companies may collect precise location data for IBA purposes. To this disclosure, the company also provided full instructions to users for disabling this collection by modifying device-level app permissions. As discussed above, WiFi Map also added a statement of adherence to the DAA Principles to its privacy disclosures. These actions provided consumers with a clear notice of the collection of this category of sensitive data and the ability to exercise choice about this third-party collection. These steps resolved WiFi Map's compliance issue under this provision of the Mobile Guidance.

Enhanced notice requirement

To resolve its compliance issues under this provision of the Mobile Guidance, WiFi Map updated its pop-up dialog to disclose to users that data, including precise location data, may be collected and shared for IBA purposes.³⁸ The dialog now includes language indicating that precise location data may be collected by third parties for IBA purposes, and points to a link that takes users to the disclosure in its privacy policy describing third-party collection of precise location data that occurs through its apps and options to disable this collection. The company also added a jump link to the top of its privacy policy, labelled "Precise Location Disclosure," that leads users to this disclosure.

Consent requirement

To come into compliance with consent requirement, as described above, WiFi Map altered its existing pop-up dialog box to contain new information about precise location data collection for IBA. As noted above, this dialogue box includes a link that takes users directly to the relevant location data collection section of its privacy policy. This section not only describes the collection of precise location data for IBA but also provides information on withdrawing consent using the operating system tools in Android and iOS. Critically, this dialog appears before the default system-level permission tool that allows users to consent (or not) to the collection of

³⁸ The Accountability Program notes that the pop-up dialog box only appears in the Android version of the app, as the third-party collection of precise location data for IBA only occurs only through this version of the app.

location data through the WiFi Map app. This permissions tool, when coupled with the compliant notice and enhanced notice provided by WiFi Map's full-screen dialog, meets the consent requirement of the Mobile Guidance. Finding that WiFi Map provided users with the ability to consent to the third-party collection of precise location data for IBA, the Accountability Program determined that this issue under the Mobile Guidance was resolved.

CONCLUSION

The mobile app space has significantly expanded from its early origins, when smartphones were considered luxury commodities. As consumers continue to enjoy the vast digital resources provided by app publishers, businesses must keep in mind their obligations to provide users with easy-to-use tools to exercise choice about digital privacy. Today, companies have a variety of means to furnish consumers with mobile privacy choices for IBA, whether through the DAA's AppChoices app or operations systems-level settings. Because of this, mobile app publishers cannot reasonably expect consumers to draft email correspondence that contains technical details and personally identifiable information in order to effectuate an opt out.

Moreover, if company allow third parties to collect precise location data through their apps for IBA, they must provide consumers with the appropriate enhanced notice and opt-in consent of this fact. Prior to collecting this type of sensitive data, companies cannot merely rely on permissions tools or full screen prompts that fail to mention third-party collection.

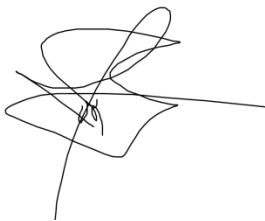
Here, WiFi Map worked diligently with the Accountability Program to meet its obligations under the Mobile Guidance, designing a bespoke dialog box explaining IBA to consumers and pointing them to the correct locations in the company's privacy policy. WiFi Map can stand as a source of emulation to mobile app developers who allow third parties to collect data through their apps for IBA. The Accountability Program applauds the company's commitment to end user privacy and industry self-regulation.

COMPANY'S STATEMENT

WiFi Map LLC would like to thank the Digital Advertising Accountability Program for bringing to our attention all the disclosure issues. Thank you for your ongoing support in ensuring our compliance. We are very pleased that we were able to correct all the issues promptly.

DISPOSITION OF DECISION

Practices voluntarily corrected.

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

Jon M. Brescia

**Vice President,
Digital Advertising Accountability Program**