

BBB NATIONAL PROGRAMS, INC.

DIGITAL ADVERTISING ACCOUNTABILITY PROGRAM

FORMAL REVIEW

Case Number: 101-2019

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

DECISION

DATE: September 5, 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 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 text of the Principles can be found at <http://www.aboutads.info/principles>.

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.”).

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

FitNow, Inc. (FitNow) is a company that publishes the mobile app Lose It! (Lose It app), an exercise and weight loss app available on the Android and iOS operating systems.⁶ The company is headquartered in Boston, Massachusetts.

INQUIRY

This case arises from the Accountability Program’s regular monitoring of mobile applications. The Accountability Program identified the Lose It app⁷ and began reviewing it for compliance with the Mobile Guidance. The Accountability Program first installed the iOS and Android versions of the app on our test devices, and was able to capture and inspect data packets being transmitted from the application. Through analysis of network traffic generated from the app, we observed third parties⁸ 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.⁹

i. Cross-app enhanced notice review

To assess FitNow’s compliance with the mobile enhanced notice requirement, the Accountability Program first examined privacy policy links on the Lose It app’s listings in the Google Play and Apple App Stores. These links directed us to the top of a privacy policy document¹⁰ for the Lose It App. 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 FitNow’s mobile app. Looking further, we could not find links to a compliant IBA disclosure either during download or

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 FitNow, <https://www.loseit.com/> (last visited April 4, 2019).

⁷ Google Play Store, *Lose It! – Calorie Counter*,

https://play.google.com/store/apps/details?id=com.fitnow.loseit&hl=en_US (last visited April 4, 2019). Apple App Store, *Lose It! – Calorie Counter*, <https://itunes.apple.com/us/app/lose-it-calorie-counter/id297368629?mt=8> (last visited April 4, 2019).

⁸ *Mobile Guidance* 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.”).

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 FitNow, *Privacy Statement and Policy* (Aug. 6, 2018), <https://www.loseit.com/privacy/> [perma: <https://web.archive.org/web/20190104214453/https://www.loseit.com/privacy/>].

upon first opening the app, which are the alternative times at which enhanced notice may be provided.

The Accountability Program looked further to determine if FitNow had provided any disclosure of third-party data collection for IBA taking place through its mobile app and examined FitNow's privacy policy for such a disclosure. While we located a discussion of third-party advertising that takes place through FitNow's services,¹¹ we noted that this language focused on advertising facilitated by cookies, which are technologies commonly used to deliver IBA in desktop environments and the mobile web.¹² The Accountability Program found that this language was not sufficiently clear to explain to consumers that third-party advertisers may collect consumer data through the Lose It app for the purpose of serving targeted ads. Looking further, the Accountability Program was unable to locate a mechanism for users to opt out of IBA occurring on mobile devices, a core requirement of the Mobile Guidance.¹³ Finally, we could not locate a statement of adherence to the DAA Principles.

ii. Precise location data collection review

During our testing of the Android version of the Lose It app, the Accountability Program observed at least one third-party company that appeared to be engaged in IBA collecting location data. The location information was in the form of latitude and longitude coordinates to the sixth and fourth decimal places, respectively, which described a point within nine meters of our testing

¹¹FitNow, *Privacy Statement and Policy* (Aug. 6, 2018), <https://www.loseit.com/privacy/> [perma: <https://web.archive.org/web/20190104214453/https://www.loseit.com/privacy/>]. (“When you visit the Websites, a cookie may be saved on your computer (if your computer accepts cookies), and if you return to the Websites the cookie may be read. A “cookie,” is a small text file placed on the user's hard drive to track usage of the Websites and collect basic information, which may include certain of your preferences. We use cookies to gain knowledge of Internet usage, improve content and advertisements, collect the site visitation data described above and in some cases to deliver specialized content... Some of our advertisers and partners occasionally use cookies as well. Lose It! does not have any control over the cookies used by advertisers and partners... Lose It! does not track its customers over time and across third party websites to provide targeted advertising and therefore does not respond to Do Not Track (DNT) signals. However, some third party sites do keep track of your browsing activities when they serve you content, which enables them to tailor what they present to you. If you are visiting such sites, your browser may be able to set the DNT signal so that third parties (particularly advertisers) know you do not want to be tracked.... Third parties that have content embedded on the Websites or App such as a social feature may set cookies on a user's browser and/or obtain information about the fact that a web browser visited the Websites from a certain IP address. Third parties cannot collect any other personally identifiable information from the Websites unless you provide it to them directly.”).

¹² The Accountability Program notes that the Mobile Web refers to the World Wide Web users can access through their smartphones and tablets using mobile web browsers. *See generally* WebWise Team, *What is the mobile web?* BBC: WebWise (Oct. 10, 2012), <http://www.bbc.co.uk/webwise/guides/mobile-web>.

¹³ FitNow, *Privacy Statement and Policy* (Aug. 6, 2018), <https://www.loseit.com/privacy/> [perma: <https://web.archive.org/web/20190104214453/https://www.loseit.com/privacy/>]. The Accountability Program notes that FitNow stated in its privacy policy that users' web browsers “may have an option that enables [the user] to disable or not accept cookies.” We note that this language is not sufficient for providing an opt-out mechanism for IBA occurring through mobile apps. The Accountability Program also notes that FitNow indicated that users could use Do Not Track (DNT) settings to signal to third-parties collecting data on websites that they “do not want to be tracked.” However, a browser-based DNT setting will not function in native apps, rendering this option unusable as a cross-app IBA opt out.

device's location.¹⁴ Believing the observed collection to be both sufficiently precise and accurate to qualify as precise location data, the Accountability Program went on to review the Lose It app for compliance with the precise location data provisions of the Mobile Guidance.

Notice review

During our review, the Accountability Program was unable to locate in FitNow's disclosures any language that provided notice of third parties' collection of precise location data for IBA, instructions for opting out of this collection, or a statement of adherence.

Enhanced notice review

During our review, 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 at any of the compliant times and locations prescribed by the Mobile Guidance.

User consent review

During our testing of the Android version of the Lose It app, we could not locate any mechanism requesting that a user consent to the collection of her precise location for IBA purposes.

Following our review, the Accountability Program sent an inquiry letter to FitNow 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

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

¹⁴ The Accountability Program has previously examined the collection of precise location data in the form of geolocation coordinates. *In re: LKQD Technologies, Inc. (77-2017)*, December 11, 2017 at 4. *See also In re: Publishers Clearing House, Inc. (92-2019)*, Jan. 28, 2019 at 2 (noting that we observed a third party collecting longitude and latitude coordinates to the seventh decimal place through the mobile app in question).

¹⁵ *Mobile Guidance* at 17.

¹⁶ *Id.*

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.

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

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 *Mobile Guidance* at 21.

¹⁹ *Id.* at 21-22.

²⁰ *Id.* at 23-24.

²¹ *Id.* § IV.A.(3)(b) at 24.

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

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, FitNow 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 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

FitNow’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.

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.

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.*

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 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.

Furthermore, when describing IBA taking place through mobile apps or engineering a mobile opt-out mechanism, companies must recognize the technical differences between IBA occurring on desktop devices versus IBA occurring through mobile apps. Opting out of cross-app IBA involves a different set of technical challenges than opting out in the web browser space. For instance, cookies are ineffective at opting consumers out of cross-app IBA because apps are walled off from one another by mobile operating systems. Mobile apps are unable to access cookie resources that have been saved to the device by a mobile web browser. The DAA Principles recognize this distinction by design, requiring that first parties provide in their disclosures descriptions of third-party cross-app IBA activity and a cross-app opt-out mechanism.

To resolve its issues under the enhanced notice provisions of the Mobile Guidance, FitNow took a number of steps. The company first updated its privacy disclosures to add a jump link to the top of its privacy policy.³⁵ This jump link directs users to a section of the FitNow privacy policy that describes third-party IBA occurring through the Lose It app that is facilitated by the collection of mobile device identifiers. This new disclosure also included a link to instructions about how to opt out of mobile IBA utilizing device-level settings³⁶ and a statement of adherence to the DAA Principles. The Accountability Program found that these actions resolved FitNow’s compliance issues under the first-party cross-app enhanced notice provisions of the Mobile Guidance.

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.

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 FitNow, *Privacy Statement and Policy* (March 21, 2019), <https://www.loseit.com/privacy/>.

³⁶ Puidokas, Whitney, *How to Opt Out of Interest Based Advertising*, <https://help.loseit.com/hc/en-us/articles/360020528073> (last visited April 4, 2019).

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 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.³⁸

During its internal compliance review process, FitNow found that it did not collect precise location data for IBA through the Lose It app or affirmatively authorize any third party to do so. However, the company found that it collected precise location data for a purpose related to the Lose It app's functionality. To ensure that no accidental exfiltration of precise location data could occur, the company pushed a patch to its mobile app that disabled the collection of this type of data entirely. The Accountability Program conducted subsequent testing of the Lose It app, which corroborated FitNow's explanation. 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 collection data through their mobile app, they must accurately disclosure this collection, and not conflate their explanations of mobile IBA with collection occurring on desktop devices that is facilitated by HTTP cookies.

Here, FitNow 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. Consumers will now have the benefits of transparency and choice when engaging with the company's exercise app.

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

³⁷ *OBA Principles* § VI. at 16–17.

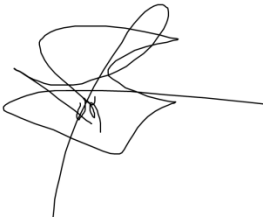
³⁸ *In re: Spinrilla (61-2016)*, May 4, 2016 (“As mobile apps are technically markedly different from websites, entities that engage in IBA through apps require specific guidance for compliance implementation that takes into account the technical issues of providing transparency and choice in the mobile 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.”).

COMPANY'S STATEMENT

FitNow is committed to respecting consumer privacy and supports the self-regulatory process. Upon receiving notice from the Accountability Program, we took immediate steps to ensure compliance with the DAA Principles, including by modifying our privacy disclosures. We thank the Accountability Program for bringing this matter to our attention and for recognizing FitNow's cooperation and compliance.

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