

BBB NATIONAL PROGRAMS

DIGITAL ADVERTISING ACCOUNTABILITY PROGRAM

COMPANY:
BPMobile LLC

CHALLENGER:
Digital Advertising Accountability Program

FORMAL REVIEW
Case Number: 120-2020

DECISION

DATE: October 8, 2020

SYNOPSIS

The Digital Advertising Alliance’s (DAA) Self-Regulatory Principles (DAA Principles)¹ cover entities engaged in interest-based advertising (IBA) across websites or mobile applications (apps). In accordance with the *Application of Self-Regulatory Principles to the Mobile Environment* (Mobile Guidance), if a mobile app publisher² allows third parties³ to collect precise location data⁴ 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. Further, mobile app publishers that authorize third parties to collect cross-app⁵ data through their apps for use in cross-app IBA must provide users with notice and enhanced notice, as described in the Mobile

¹ The DAA Principles include a suite of four documents related to interest-based advertising available at <http://www.aboutads.info/principles>. The relevant documents are: *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).

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

³ *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.”).

⁴ *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.”).

⁵ *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.”).

Guidance. DAA codes of conduct are independently enforced by the Digital Advertising Accountability Program (Accountability Program), a division of BBB National Programs.⁶

COMPANY STATUS

BPMobile LLC (BPMobile) is a mobile app publisher that specializes in utility and business apps. The company is based out of Minsk, Belarus. The company's apps are available in both the Apple App Store and Google Play Store,⁷ and its iScanner: Free Portable PDF Scanner App (iScanner) has approximately 10,000,000 downloads in the Google Play Store.

INQUIRY

This case arises from the Accountability Program's regular monitoring activities.

i. Location data compliance review

The Accountability Program examined BP Mobile's mobile application iScanner, which is available on the Android and iOS operating systems.⁸ As part of our investigation, we downloaded and installed iScanner on our test devices. During our testing of the iOS version of iScanner, the Accountability Program observed at least one 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 which described points within 22 meters of our testing device's location.⁹ The Accountability Program believed the observed collection to be both sufficiently precise and accurate to qualify as precise location data, triggering the notice,

⁶ See generally, BBB National Programs, *Digital Advertising Accountability Program*, <https://www.bbbprograms.org/programs/all-programs/daap/> (last visited May 26, 2020).

⁷ Google Play Store, *iScanner: Free Portable PDF Scanner App*, https://play.google.com/store/apps/details?id=com.bpmobile.iscanner.free&hl=en_US (last visited Sept. 17, 2020); Apple App Store, *iScanner: PDF Document Scanner*, <https://itunes.apple.com/us/app/iscanner-pdf-document-scanner/id1035331258?mt=8> (last visited Sept. 20, 2020); Google Play Store, *Second Phone Number: private texting & calling app*, https://play.google.com/store/apps/details?id=com.bpmobile.second.phone&hl=en_US (last visited Sept. 1, 2020); Apple App Store, *Second Phone Number*, <https://apps.apple.com/us/app/second-phone-number/id1216135390> (last visited Sept. 1, 2020); Google Play Store, *Fax from Phone Free - Fax App*, https://play.google.com/store/apps/details?id=com.bpmobile.ifax.free&hl=en_US (last visited Sept. 1, 2020); Apple App Store, *Fax App- Send Fax from iPhone*, <https://apps.apple.com/us/app/fax-from-iphone-send-fax-app/id1135811739> (last visited Sept. 1, 2020); Apple App Store, *Secret Photo Album - SA*, <https://apps.apple.com/us/app/secret-photo-album-sa/id1174964304> (last visited Sept. 2, 2020); Apple App Store, *Call Record App*, <https://apps.apple.com/us/app/call-recorder-app/id1200776424> (last visited Sept. 1, 2020); Apple App Store, *Safe24: Find My Family & Phone*, <https://apps.apple.com/us/app/find-my-friends-phone-tracker/id1348649804> (last visited Sept. 1, 2020).

⁸ *Id.*

⁹ *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."). The Accountability Program has previously examined the collection of precise location data in the form of geolocation coordinates. See, e.g., *In re: LKQD Technologies, Inc. (77-2017)*, December 11, 2017 at 4 available at <https://www.bbb.org/globalassets/local-bbbs/council-113/media/behavioral-advertising/lkqd-decision.pdf>; *In re: Spinrilla (61-2016)*, May 4, 2016 at 2 available at <https://www.bbb.org/globalassets/local-bbbs/council-113/media/behavioral-advertising/spinrilla-decision.pdf>.

enhanced notice, and consent requirements of the Mobile Guidance.¹⁰ The Accountability Program then assessed BPMobile for compliance with these provisions.

Notice review

The Accountability Program located language in BPMobile’s privacy disclosures for iScanner indicating that location data may be collected and transferred to third parties for IBA purposes.¹¹ However, we were unable to locate a tool for providing or withdrawing consent regarding the collection of precise location data or a statement of adherence to the DAA Principles.¹²

Enhanced notice review

The Accountability Program assessed whether BPMobile had provided any enhanced notice of third-party collection of precise location data for IBA. During its review, the Accountability Program was unable to locate any enhanced notice disclosure or link of third-party precise location data collection in any of the compliant locations, raising an issue under this provision of the Mobile Guidance.

User consent review

During our testing of the iOS version of the iScanner, we could not locate any mechanism requesting that a user consent to the collection of her precise location for IBA purposes. Notably, during our testing of the iOS version of iScanner, we did not observe any permissions tool—not even the default system permissions prompts—whereby a user could consent to the collection of their location data for any purpose, despite this apparent background data collection occurring.

Other mobile apps’ compliance with precise location provisions

The Accountability Program reviewed BPMobile’s other mobile app offerings for compliance with the precise location data provisions of the Mobile Guidance, and found that third parties were also collecting geolocation data coordinates through the app Secret Photo Album Vault (Secret Photo), likely for IBA.¹³ We noted that these coordinates also specified a point in space

¹⁰ *Mobile Guidance* § IV at 21-30. See generally *In re: Publishers Clearing House, Inc.* (92-2019), January 28, 2019 available at <https://www.bbb.org/globalassets/local-bbbs/council-113/media/behavioral-advertising/publishers-clearing-house-decision.pdf>; *In re: Finish Line, Inc.* (86-2018), September 26, 2018 available at <https://www.bbb.org/globalassets/local-bbbs/council-113/media/behavioral-advertising/finish-line-decision.pdf>.

¹¹ BPMobile, *Privacy Policy* (February 2019), <http://bpmob.com/scannerfree/privacy/en> [perma: <https://web.archive.org/web/20190507145817/http://bpmob.com/scannerfree/privacy/en/>].

¹² As discussed in the section of this document regarding cross-app data collection, BPMobile’s disclosures for iScanner provided instructions on how to opt out of “marketing tracking” by utilizing device-level settings. During testing, the Accountability Program engaged the “Limit Ad Tracking” setting on its iOS device and found that third-party companies persisted in collecting precise location data through the app.

¹³ BP Mobile, *Secret Photo Album Vault*, <https://itunes.apple.com/us/app/secret-photo-album-vault/id1174964304?mt=8> (last visited April 17, 2019). See also BP Mobile, *Privacy Policy* (May 25, 2018) <https://bpmob.com/secretalbumfree/privacy/en/>. The Accountability Program notes that during our testing of Secret Photo we did not observe any permissions tool—not even the default system permissions prompts—whereby a user could consent to the collection of their location data for any purpose.

within 22 meters of our test device's location. During our review of Secret Photo, we observed the same compliance issues with respect to notice, enhanced notice, and consent.

ii. Cross-app compliance review

The Accountability Program examined iScanner for compliance with the cross-app provisions of the Mobile Guidance. During our tests, we were able to capture and inspect data packets being transmitted from the Android and iOS versions of the app. Through analysis of network traffic generated from the app, we observed third parties collecting cross-app¹⁴ data, likely for IBA. Specifically, we noted the collection of Android's Advertising ID (AAID or IFA) and Apple's Identifier for Advertising (IDFA).¹⁵

The Accountability Program went on to examine iScanner's compliance with the mobile enhanced notice requirement for cross-app data. While testing the both versions of iScanner, the Accountability Program was unable to find an enhanced notice link in any of the times or locations required by the Mobile Guidance. While iScanner provided a link to the top of a privacy policy document¹⁶ within its listing on the Google Play and Apple App Stores, this type of link did not function as an enhanced notice link. This is because it did not take users directly to a disclosure that describes the third-party IBA activity BPMobile allows through its app.¹⁷ While we noted that the Android version of iScanner provided a "privacy notice" screen pointing users to a privacy policy link, this screen also did not function to enhanced notice, as it did not direct users to an IBA disclosure. We could find no other link that would serve as enhanced notice under the Mobile Guidance.

The Accountability Program additionally reviewed a number of BPMobile's other app offerings and identified the same enhanced notice compliance issue.

Looking for disclosure of third-party data collection for IBA, the Accountability Program found that BPMobile had provided a number of different privacy policies for its mobile apps.¹⁸ In most

¹⁴ *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.").

¹⁵ 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.").

¹⁶ BPMobile, *Privacy Policy* (February 2019), <http://bpmob.com/scannerfree/privacy/en> [perma: <https://web.archive.org/web/20190507145817/http://bpmob.com/scannerfree/privacy/en/>].

¹⁷ *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).

¹⁸ BPMobile, *Privacy Policy* (February 2019), <http://bpmob.com/scannerfree/privacy/en> [perma: <https://web.archive.org/web/20190507145817/http://bpmob.com/scannerfree/privacy/en/>]; BPMobile, *Privacy Policy* (May 25, 2018), <https://bpmob.com/secretalbumfree/privacy/en/>; BPMobile, *Privacy Policy*, <http://bpmob.com/sp-android/free/privacy/en/> (last visited April 25, 2019) [perma: <https://perma.cc/VX6G-VPD5>]; BPMobile, *Privacy Policy* (May 25, 2019), <https://bpmob.com/sp/free/privacy/en/> [perma: <https://web.archive.org/web/20190629093236/https://bpmob.com/sp/free/privacy/en/>]; BPMobile, *Privacy Policy* (May 25, 2018), <http://bpmob.com/fax/privacy/en/> [perma: <https://web.archive.org/web/20190303094954/http://bpmob.com/fax/privacy/en/>]; BPMobile, *Privacy Policy* (May 25, 2019), <http://bpmob.com/callrecorderfree/privacy/en/> [perma: <https://web.archive.org/web/20181226013816/http://bpmob.com/callrecorderfree/privacy/en/>]; BPMobile, *Privacy*

of these privacy policies we located a disclosure indicating that third parties may collect data through each application for IBA purposes, as well as instructions on how to access device-level settings to opt out of mobile IBA.¹⁹ However, we could not locate a statement of adherence to the DAA Principles in any of these documents.

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

ISSUES RAISED

i. Precise location data requirements

Notice requirement

According to section IV.A.(1) of the Mobile Guidance, first parties must provide clear, meaningful, and prominent notice when they affirmatively authorize third parties to collect precise location data for use in IBA from or through their application(s).²⁰ 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.²¹

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).²² 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.²³ 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.²⁴ Companies may use the

Policy (March 2019), <https://bpmob.com/safe24/privacy/en/> [perma: <https://web.archive.org/web/20190610093343/https://bpmob.com/safe24/privacy/en/>]; BPMobile, *Privacy Policy* (May 25, 2018), <http://bpmob.com/faxfree/privacy/en/>.

¹⁹ The Accountability Program notes that the Android version of iScanner had an option within its settings that appeared to allow users to select an option to "Personalize ad experience." At the time of our review, when we toggled the setting to what appeared to be the "off" switch we continued to observe the collection of our device's IFA by third parties known to engage in IBA. In reviewing the network traffic generated by this app, we could find no evidence that this tool stopped the third-party use of device identifiers for IBA.

²⁰ *Mobile Guidance* at 21.

²¹ *Id.* at 21-22.

²² *Id.* at 23-24.

²³ *Id.* § IV.A.(3)(b) at 24.

²⁴ *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.").

mechanisms provided by the application store to fulfill this notice requirement.²⁵ 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.²⁶

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.²⁷ This consent tool should be easy to use and should apply to the application and device from which the consent is provided.²⁸ The first party is also required to provide an easy-to-use tool for withdrawing consent at any time.²⁹ Under the Mobile Guidance, valid consent requires an action in response to a “clear, meaningful, and prominent notice.”³⁰ 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.³¹ A company may also use permissions tools provided by an application platform or application market provider to satisfy this requirement.³²

ii. 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.³³ 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.³⁴

²⁵ *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.

²⁶ *Id.* at 23.

²⁷ *Id.* at 25-26.

²⁸ *Id.* § IV.B.(1)(a) at 25.

²⁹ *Id.* § IV.B.(1)(b) at 26.

³⁰ *Mobile Guidance* Definition B at 4.

³¹ *Id.* Commentary to § IV.B.(1) at 27. The application settings may only be used by the first party to satisfy this requirement if provides notice of transfer of location data to a third party.

³² *Id.*

³³ *Mobile Guidance* at 17.

³⁴ *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, *First Party Enhanced Notice 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_2 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.”).

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 or links to the privacy policies of third-party partners.³⁵

COMPANY RESPONSE AND ANALYSIS

Once a line of communications was firmly established with the Accountability Program, BPMobile took several steps to resolve the issues identified in the Accountability Program's inquiry letter, discussed below:

i. Compliance with precise location data requirements

The DAA Principles recognize the distinction between the use of standard data types for IBA versus more sensitive data like financial or medical information.³⁶ The Mobile Guidance reserves those norms of sensitivity and recognizes 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.³⁷

Following receipt of the Accountability Program's inquiry letter, BPMobile appeared to disable the third-party collection of precise location data across its apps. Subsequently, the Accountability Program conducted several rounds of testing of the company's app products and found that third parties were no longer collecting precise location data for IBA purposes. BPMobile then confirmed to the Accountability Program that this collection was no longer occurring in its products. 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.

ii. Compliance with cross-app requirements

BPMobile's authorization of third-party collection of unique identifiers for IBA in its mobile apps triggered compliance responsibilities under the first-party cross-app provisions of the Mobile Guidance. Consequently, BPMobile should have provided an enhanced notice link to a

³⁵ DAA, *AppChoices*, <https://youradchoices.com/appchoices> (last visited Nov. 12, 2019).

³⁶ *OBA Principles* § VI, at 16–17.

³⁷ *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.”).

compliant cross-app IBA disclosure. However, at the time of our inquiry BPMobile provided no enhanced notice link and a partially-compliant IBA disclosure.

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

As detailed above, the cross-app provisions of the Mobile Guidance prescribe particular times and locations where consumers can receive enhanced notice that directs them to a compliant IBA disclosure.³⁸ 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.³⁹ 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.⁴⁰ This ensures that when a user taps on a privacy policy link in an app store listing, they are directed immediately to relevant information about IBA and an opt-out mechanism.

To achieve compliance in this way, BPMobile published a new set of privacy policies for its apps that includes an IBA-specific jump link at the top of each document.⁴¹ This jump link, accompanied by the language “Interest based advertising: to learn more about data disclosure [click here](#),” directs users to a section of the relevant policy that describes third-party IBA occurring through BPMobile’s apps. This IBA disclosure includes a statement of adherence to the DAA Principles and lists each of BPMobile’s third-party ad partners with links to their privacy policies. BP Mobile also added an additional jump link, entitled “DO NOT USE MY DATA” that directs users to instructions on accessing OS-level settings for opting out of mobile IBA and a link to the industry-developed page youradchoices.com.

Now, when consumers tap on the privacy policy links for BPMobile’s apps’ pages in the app stores, they will be able to immediately access information about IBA. The Accountability

³⁸ *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.

³⁹ *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.”).

⁴⁰ *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).

⁴¹ BPMobile, *Privacy Policy* (July 20, 2020), <http://bpmob.com/scannerfree/privacy/en/>; BPMobile, *Privacy Policy* (March 2020), <http://bpmob.com/sp-android/free/privacy/en/>; BPMobile, *Privacy Policy* (March 2020), <https://bpmob.com/sp/free/privacy/en/>; BPMobile, *Privacy Policy* (March 2020), <http://bpmob.com/faxfree/privacy/en/>; BPMobile, *Privacy Policy* (March 2020), <http://bpmob.com/fax/privacy/en/>; BPMobile, *Privacy Policy* (March 2020), <https://bpmob.com/salbumfree/privacy/en/>; BPMobile, *Privacy Policy* (January 2020), <https://bpmob.com/safe24/privacy/en/>.

Program found that these actions, taken together, resolved BP Mobile's compliance issues under the first-party cross-app enhanced notice provisions of the Mobile Guidance.

CONCLUSION

Today's case follows a long line of Accountability Program enforcement actions that highlight the importance of meeting the Mobile Guidance's requirements when authorizing the third-party collection of precise location data. App publishers should recognize the sensitivity surrounding a user's precise location data and fashion their business practices accordingly when choosing to use or share this type of data. Today's case also underscores the requirements for app and website publishers to provide users with enhanced notice about third-party cross-app data collection occurring on their properties. First parties must provide a timely, up-front notice to users about this background data collection of their device identifiers.

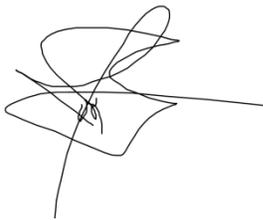
The Accountability Program applauds BPMobile for its actions to meet best practices for data privacy and IBA. We appreciate the company's support of industry self-regulation.

COMPANY'S STATEMENT

BPMobile declined to provide a company statement.

DISPOSITION OF DECISION

Practices voluntarily corrected.

A handwritten signature in black ink, appearing to read 'Jon M. Brescia', written over a faint rectangular box.

Jon M. Brescia
Vice President
Digital Advertising Accountability Program