



provide notice, enhanced notice, and an easy-to-use opt-out mechanism to meet the requirements of the guidance provided in the DAA’s Mobile Guidance. Companies that collect precise location data through mobile apps for IBA must comply with another set of third-party provisions of the Mobile Guidance, including obtaining users’ opt-in consent for this collection. When they are technologically limited from obtaining users’ consent directly, they must take steps to obtain reasonable assurances of compliance from their first-party<sup>4</sup> partners. The Cross-Device Guidance requires companies that collect data across multiple devices and associate this data with a particular user to provide notice of this practice and explain the scope of the choice provided on each device. Finally, companies that make representations to consumers about the use of their data must comply with the Material Changes provision of the OBA Principles.

## COMPANY STATUS

Kiip, Inc. (Kiip) is an advertising technology company headquartered in San Francisco, California.

## INQUIRY

In the course of its regular monitoring activities, the Accountability Program selected a number of popular applications on the iOS and Android operating systems to review for first- and third-party compliance with the DAA Principles. These applications included the popular health and fitness app, Sweatcoin, available on the Android and iOS operating systems and published by SweatCo Ltd.<sup>5</sup> The Accountability Program observed that Kiip was collecting user data for IBA through this app, likely for IBA, prompting us to review the company’s practices for compliance with the DAA Principles. Below, we describe our review in detail.

### I. Mobile data collection review

#### i. Cross-app data review

As part of our investigation, the Accountability Program downloaded and installed Sweatcoin on our testing devices. Using our testing equipment, we were able to capture and inspect IP packets being transmitted from the application. Through analysis of the application’s network traffic, we

---

non-affiliate websites or entities, *OBA Principles* Definition J at 11 (“An entity is a Third Party to the extent that it engages in Online Behavioral Advertising on a non-Affiliate’s Web site.”).

<sup>3</sup> *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.”).

<sup>4</sup> The term “first party” can refer to both the publisher of a mobile application, *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.”), and the owner and operator of a website and its affiliates, *OBA Principles* Definition F at 10 (“A First Party is the entity that is the owner of the Web site or has Control over the Web site with which the consumer interacts and its Affiliates.”).

<sup>5</sup> Google Play Store, *Sweatcoin Pays You To Get Fit*, <https://play.google.com/store/apps/details?id=in.sweatco.app> (last visited Aug. 29, 2018); Apple App Store, *Sweatcoin – Sweat for Coin*, <https://itunes.apple.com/us/app/sweatcoin-sweat-for-coin/id971023427> (last visited Sept. 4, 2018).

observed Kiip collecting cross-app data, likely for IBA.<sup>6</sup> Specifically, the Accountability Program noted the collection of our device’s Apple Identifiers for Advertisers (IDFA) value—a unique alphanumeric string used to identify a particular device for advertising purposes.<sup>7</sup>

#### A. *Third-party notice*

The Accountability Program navigated to Kiip’s website to assess its compliance with the notice obligations of the Mobile Guidance. We first examined the company’s privacy policy, which we accessed through a link on the company’s footer labelled “Privacy Policy.” Scrolling through this policy, we located a description of Kiip’s IBA practices:

We receive and store any information you enter on our Platform or provide to us in any other way. The types of Personal Information collected may include your email address, IP address, latitude and longitude, browser or mobile device information, and any other information necessary for us to provide our services. ... The Personal Information you provide is used for such purposes as ... customizing the advertising and content you see....<sup>8</sup>

We noted that the privacy policy also contained some language describing users’ ability to opt out of IBA through three separate opt-out mechanisms. First, the policy included a link to a dedicated opt-out page for Kiip’s IBA.<sup>9</sup> It went on to say that “for more opt-out options” users could download the DAA’s AppChoices App. Finally, the policy described the fact that users could opt out of “most in-app mobile online behavioral advertising” by utilizing operating system-level settings, and provided brief instructions for finding these settings (which, if followed, would only lead users to the correct settings on some versions of the operating systems described).<sup>10</sup> The policy also included a statement of adherence to the DAA Principles.

The Accountability Program went on to examine Kiip’s dedicated opt-out page, as linked from the privacy policy. We found that this page was a facsimile of Kiip’s full privacy policy with one exception: the opt-out page contained additional language informing users that they could opt out of Kiip’s own IBA by entering a “Device Advertising ID” into a text-entry field and clicking on a button labelled “Opt Out.”

---

<sup>6</sup> *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.”).

<sup>7</sup> See IAB Mobile Marketing Center of Excellence, *Mobile Identity Guide for Marketers* at 4, June 2017, <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.”).

<sup>8</sup> Kiip, *Privacy Policy* (May 2, 2016), <https://api.kiip.me/privacy/> (archived at <https://web.archive.org/web/20160212161935/https://app.kiip.me/privacy/>).

<sup>9</sup> *Id.* (“To opt-out of Kiip’s in-app mobile online behavioral advertising practices as detailed in this Privacy Policy, visit <http://app.kiip.me/optout/all>.”).

<sup>10</sup> *Id.* (“On Apple devices, the setting may be under Settings-Privacy-Advertising-Limit Ad Tracking. On Android devices, the setting may be under Settings-Account & Sync-Google-Ads-Opt Out of Interest-Based Ads.”).

The Accountability Program appreciated that Kiiip’s privacy notices included disclosures describing its IBA practices, a statement of adherence to the DAA Principles, and a range of tools for users to exercise choice about IBA. However, we had compliance concerns about the clarity of Kiiip’s descriptions of all three of the choice mechanisms it provided to users:

- Kiiip’s description of and accompanying instructions for its text-entry device ID opt-out mechanism did not provide users with sufficient information to easily register their choice to opt out. This raised a number of concerns related not only to the clarity of the notice but also to whether the opt out itself met the easy-to-use standard required by the DAA Principles.<sup>11</sup> First, the opt out required that users manually enter their “Device Advertising ID” into a text field without providing users with a definition of this term. Further, the opt-out tool lacked any format verification mechanism to assist users in the event of an error in their manual entry. Finally, the opt-out page did not provide instructions to users on how to obtain their device ID on common mobile operating systems. Taken together, these deficiencies showed that Kiiip’s disclosures were unlikely to assist the average user in opting out.
- While Kiiip pointed users to the DAA’s AppChoices app, we noted Kiiip was not listed among the participating companies in the AppChoices app. Therefore, the presence of a link to download this app was not a clear description of an easy-to-use choice mechanism for Kiiip’s IBA under the Mobile Guidance.
- We noted that Kiiip pointed users to OS-level device settings for users to opt out of IBA on mobile devices. However, these instructions merely indicated that users could opt out of “*most* in-app mobile online behavioral advertising” (emphasis added) through using these features and did not specify whether Kiiip itself honored these settings.

#### *B. Third-party enhanced notice*

The Accountability Program went on to assess whether Kiiip had ensured that users were provided with enhanced notice of its third-party IBA practices when using the first-party app. When downloading, installing, and using the Sweatcoin application, we checked for the presence of compliant enhanced notice, either provided by Kiiip in or around any ads delivered through the app or provided by the app publisher. However, we could find no such notice being provided by Kiiip or the first-party publisher during our tests.

- ii. Precise location data review

---

<sup>11</sup> The Accountability Program previously found a mobile opt-out mechanism overly cumbersome in a case covering the company Adbrain, where the company required that users obtain a “device ID” without any meaningful instructions about how to do so and enter it, without error, into a text entry field. This case is discussed below in the compliance analysis section of this document.

The Accountability Program observed the collection of location data by Kiip through the Sweatcoin application. Specifically, we observed that the data Kiip collected included latitude and longitude coordinates to the fourteenth decimal place.<sup>12</sup>

#### A. *Third-party notice*

During our review of Kiip’s privacy disclosures, we noted that Kiip’s privacy policy included language about the collection of “latitude and longitude” coordinates for purposes including “customizing the advertising and content [a user] sees.”<sup>13</sup> The Accountability Program appreciated that Kiip referenced the collection of precise location data for targeted advertising purposes in its privacy disclosures. However, we could not locate instructions for users to provide or withdraw consent regarding the collection and use of their precise location data for IBA.

#### B. *Third-party consent*

During testing, we examined the Sweatcoin application to determine if either Kiip or the first-party application publisher requested consent for the third-party collection and use of precise location data for IBA. While we noted during testing that Sweatcoin requested permission through the operating system’s permissions tool and through an in-app notice to use the device’s location, this appeared insufficient for purposes of compliance with the opt-in consent requirement of the Mobile Guidance. This is because neither the in-app notice nor the permissions request dialogue mentioned the collection of precise location data by third parties, generally, or Kiip specifically, or explained the intended use of this data for third-party IBA.

## II. Multi-site data review

The Accountability Program went on to assess Kiip’s compliance with the desktop-based OBA Principles.<sup>14</sup> During our review of Kiip’s privacy disclosures, we noted the language stating that “Users are bound by any changes to the Privacy Policy when he or she uses the Platform after such changes have been first posted.”<sup>15</sup> The Accountability Program found that this language was ambiguous as to Kiip’s compliance with the Material Changes provision of the OBA Principles

---

<sup>12</sup> *Mobile Guidance* Definition K at 9 (“Precise Location Data is data obtained from a device about the physical location of a 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. *In re: LKQD Technologies, Inc. (77-2017)*, December 11, 2017 at 4. *See also In re: Spinrilla (61-2016)*, May 4, 2016 at 2 (noting that we observed a third party collecting longitude and latitude coordinates to the fourteenth decimal place through the mobile app in question).

<sup>13</sup> Kiip, *Privacy Policy* (May 2, 2016), <https://api.kiip.me/privacy/> (archived at <https://web.archive.org/web/20160212161935/https://app.kiip.me/privacy/>).

<sup>14</sup> *OBA Principles* Summary at 2 (“The Principles apply to online behavioral advertising, defined as the collection of data online from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors.”).

<sup>15</sup> Kiip, *Privacy Policy* (May 2, 2016), <https://api.kiip.me/privacy/> (archived at <https://web.archive.org/web/20160212161935/https://app.kiip.me/privacy/>).

as it did not include information about whether material changes to privacy practices could be applied retroactively to data previously collected.

### **III. Cross-device data review**

During the Accountability Program’s review of the Kiip website, we observed language that appeared to indicate that Kiip was engaged in the collection and association of data across devices for IBA. Specifically, we noted that Kiip stated in its privacy disclosures that the company may “also provide Personal Information and/or aggregate data to those partners for remarketing purposes, cross device analysis and for monitoring performance metrics.”<sup>16</sup> We also noted that in the section of Kiip’s website describing its “Moments Data Stream” line of businesses, the company states that “[m]illions of our device IDs are linked to an email address, which maps data to a verified user and maximizes cross-device opportunities.”<sup>17</sup> This language suggested that Kiip was engaged in the collection and use of data across devices for IBA purposes. When coupled with the lack of language in Kiip’s disclosures addressing the scope of the company’s opt-tools in the context of cross-device linking, this raised a possible compliance issue under the Cross-Device Guidance.

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

## **ISSUES RAISED**

### **I. Requirements under the Mobile Guidance**

The Mobile Guidance adapts the desktop-oriented rules of the OBA Principles to the mobile world, including the core requirements for third parties to provide transparency and consumer control for IBA. As a collector and user of data for IBA across non-affiliate applications, Kiip is a third party under the Mobile Guidance. Third parties may have multiple separate transparency and control responsibilities depending on the types of data they collect.

#### **i. Cross-app data**

##### **A. *Third-party notice requirement***

Under section III.A.(1) of the Mobile Guidance, third parties who engage in the collection or use of cross-app data for IBA must provide a clear, meaningful, and prominent notice on their websites or accessible from the applications that host them.<sup>18</sup> This notice must include (1) the types of data collected, (2) the uses of such data, (3) an easy-to-use mechanism for exercising

---

<sup>16</sup> Kiip, *Privacy Policy* (May 2, 2016), <https://api.kiip.me/privacy/> (archived at <https://web.archive.org/web/20160212161935/https://app.kiip.me/privacy/>).

<sup>17</sup> Kiip, *Introducing Moments Data Stream*, <http://www.kiip.me/moments-data/> (last visited March 26, 2018).

<sup>18</sup> *Mobile Guidance* at 14.

choice with respect to the collection and use of such data or the transfer of such data to a non-affiliate for IBA, and (4) the fact the third party adheres to the DAA Principles.<sup>19</sup>

### *B. Third-party enhanced notice requirement*

As a complement to the notice requirement of section III.A.(1) of the Mobile Guidance, section III.A.(2) requires third parties to provide enhanced notice to users of cross-app data collection by ensuring that users receive a clear, meaningful and prominent link to the III.A.(1) disclosure.<sup>20</sup> This link must be presented in or around an advertisement delivered using cross-app data.<sup>21</sup> Alternatively, the link may be presented (1) before the application is installed, as part of the process for downloading the application, at the time the application is opened for the first time, or at the time cross-app data is first collected, and (2) in the application's settings or any privacy policy.<sup>22</sup>

### *C. Third-party consumer control requirement*

Under section III.B.(1) of the Mobile Guidance, third parties must provide users with the ability to exercise choice with respect to their collection and use of cross-app data for IBA. Such choice should be described in the notice required under section III.A. of the Mobile Guidance, described above.<sup>23</sup>

#### ii. Precise location data

### *A. Third-party notice requirement*

Under section IV.A.(2) of the Mobile Guidance, a third party must give clear, meaningful, and prominent notice of the collection and use of precise location data for IBA or the transfer of precise location data to it for its use in IBA.<sup>24</sup> Such notice should include (1) the fact precise location data is collected, (2) the uses of such data, (3) instructions for providing or withdrawing consent for the collection and use of precise location data, **and** (4) the fact the company adheres to the DAA Principles.<sup>25</sup> A third party should provide such notice on its own website or through the first-party application through which it is collecting precise location data.<sup>26</sup>

### *B. Third-party consent requirement*

---

<sup>19</sup> *Id.*

<sup>20</sup> *Id.* at 14-15.

<sup>21</sup> *Id.* at 15.

<sup>22</sup> *Id.* First and third parties each have an independent responsibility to ensure that enhanced notice is provided through one of the compliant means. See the Company Response and Analysis section, below, for further discussion of this requirement.

<sup>23</sup> *Mobile Guidance* at 18-19.

<sup>24</sup> *Id.* at 22.

<sup>25</sup> *Id.* at 22-23.

<sup>26</sup> *Id.*

Under section IV.B.(2) of the Mobile Guidance, a third party should obtain consent<sup>27</sup> from a user prior to collecting or using precise location data for IBA purposes or get reasonable assurances that the first party has obtained consent for the third party's collection and use of precise location data for IBA.<sup>28</sup>

## **II. Requirements under the OBA Principles**

The OBA Principles govern the collection of multi-site data across websites for IBA. Under section V. of the OBA Principles, covered entities should acquire users' consent before making material changes to their IBA data use policies or practices.<sup>29</sup> Specifically, a company must obtain opt-in consent if (1) it makes a material change to its IBA practices resulting in more expansive uses of data than previously disclosed to the user, *and* (2) the company applies this material change retroactively to data previously collected from the user under an earlier version of its privacy policy.

## **III. Requirements under the Cross-Device Guidance**

The Cross-Device Guidance clarifies how companies who reach consumers across their various digital devices should provide them with notice and choice about IBA.<sup>30</sup>

### *A. Transparency*

Under the Transparency provision of the Cross-Device Guidance, a company that associates or links data collected from multiple devices for IBA must provide a notice either (1) on its website or (2) accessible from applications where it collects data for IBA that explains these practices.<sup>31</sup>

---

<sup>27</sup> See *id.* Definition B at 4 (“Consent means an individual’s action in response to a clear, meaningful, and prominent notice regarding the collection and use of data for a specific purpose. Where an entity has a relationship with a consumer through an additional or different medium than the device to which Consent applies, Consent may be obtained through any such medium.”).

<sup>28</sup> *Id.* § IV.B.(2) at 29 (“A Third Party obtains reasonable assurances...if the Third party takes measures such as: (1) entering into a contract with the First party under which the First Party agrees to obtain Consent to the Third Party’s data collection and use; (2) obtaining other written assurances from the First Party to the same effect; (3) conducting periodic checks or audits of the First Party’s consent practices (4) verifying that the First Party publicly represents that it obtains Consent to the transfer of Precise Location Data to a Third Party....”).

<sup>29</sup> *OBA Principles* Section V. at 16 (“Entities should obtain Consent before applying any material change to their Online Behavioral Advertising data collection and use policies and practices prior to such material change.”).

<sup>30</sup> See *Compliance Warning: February 1, 2017, Enforcement of Cross-Device Guidance (CW-04-2017)*, Feb. 1, 2017, <https://www.bbb.org/globalassets/local-bbbs/council-113/media/behavioral-advertising/compliance-warning-cw-04-2017-cross-device-enforcement.pdf> (“As consumers move seamlessly across smartphone, tablet, laptop, and desktop, the IBA ecosystem has developed new ways of collecting and using data to serve IBA across these multiple devices. Cross-device IBA allows companies to learn about a consumer’s interests on one device and show them ads relevant to those interests on other devices. Depending on the technology available to the company, the identity of the consumer or device is either ‘probabilistic,’ that is, based on a number of factors that link a user or related users who share devices, or ‘deterministic,’ that is, based on a user’s sign-in or other method of self-identification across devices.”). See also *In re: LKQD Technologies, Inc. (77-2017)*, December 11, 2017 at 8.

<sup>31</sup> *Cross-Device Guidance* at 3-4. The requirements of this notice are described more fully in footnote 4 (explaining that “this notice should be provided on a Third Party’s own Web site(s) or accessible from application(s) from or through which they collect Cross-App Data (see OBA Principles at p. 12; Mobile Guidance at p. 14). This notice should also indicate the Third Party’s collection and use of Precise Location Data for use across devices. Consent for

This notice must include a description of a choice mechanism for users to opt out of IBA and accurately explain the scope of the company’s opt out.<sup>32</sup>

### *B. Consumer control*

Whether on desktop or mobile devices, companies must provide consumers with a means to opt out from IBA. The Consumer Control provision of the Cross-Device Guidance explains how opting out functions in the context of cross-device IBA. According to this guidance, companies should not collect browsing or app usage data from the opted-out device for use in IBA on that device or on a linked device; this includes transferring the data to another third party for its use in IBA.<sup>33</sup> Companies also should not use data collected on a consumer’s other linked devices to serve IBA on the opted-out device. Companies are free to expand the scope of their opt outs to cover all devices linked to the device from which a consumer opts out.<sup>34</sup> However, the Cross-Device Guidance does not require this expansive opt-out scope.<sup>35</sup> Rather, companies may continue to treat opt outs as applying only to a particular browser or device. Whichever method a company chooses, it must be sure to explain clearly the scope of the opt out in its disclosure described under the transparency section of the Cross-Device Guidance so that consumers are apprised of the effect their opt-out decision will have. Finally, we note that a consumer’s decision to opt out affects data collection and use going forward. Data collected from a device prior to opting out is not affected by the opt-out decision.<sup>36</sup>

## **COMPANY RESPONSE AND ANALYSIS**

Following receipt of the Accountability Program’s inquiry letter, Kiip demonstrated its commitment to achieving full compliance with the DAA Principles and immediately conducted a thorough review of its data collection practices. The company swiftly provided the Accountability Program with detailed descriptions of its practices and consulted with the Accountability Program on its plan to come into compliance with the DAA Principles.

### **I. Compliance with the Mobile Guidance**

#### **i. Cross-app data**

Kiip’s collection of device identifiers for IBA through mobile apps triggers its responsibilities under the third-party cross-app provisions of the Mobile Guidance.

---

the collection and use of Precise Location Data should encompass the collection of Precise Location Data from a device for use on another computer or device that is linked to the device where Consent is obtained.”).

<sup>32</sup> *Id.* For more information about the scope of opt outs in a cross-device context, see the next section on the Consumer Control provision of the Cross-Device Guidance.

<sup>33</sup> *Id.* at 4.

<sup>34</sup> *Id.* at 4, n.8.

<sup>35</sup> Not all companies are technically capable of providing opt outs across all linked devices. Particularly with regard to probabilistic methodologies, a cross-device opt out could be either under- or over-inclusive. Moreover, some consumers may wish to opt out of IBA on a particular device, such as their office laptop, but want to receive ads based on their preferences on other devices.

<sup>36</sup> *Id.*

### A. Third-party notice requirement

The Mobile Guidance mandates that companies provide consumers with a notice of their cross-app IBA practices that includes a clear description of an easy-to-use choice mechanism. Critically, these requirements recognize that in today’s digital marketplace users display a range of levels of technical sophistication. Thus, each company must not only provide an easy-to-use opt-out tool, but also describe this tool in a clear and meaningful way such that ordinary consumers can easily opt out of the company’s IBA practices if they so choose. The Accountability Program discussed these requirements at length in our *Adbrain* decision.<sup>37</sup>

Similarly, at the time of the Accountability Program’s review, Kiip’s privacy disclosures did not provide clear instructions that could render their opt-out tool easy to use. An opt out can only be “easy to use” if an ordinary consumer is able to effectuate the opt out by following the instructions that the company provides. As we indicated in our *Adbrain* decision, instructions to consumers should be “complete, correct, and comprehensible.”<sup>38</sup>

The single opt-out tool that Kiip specified in its disclosures could be used to halt its own IBA practices—a text box submission field requesting that users manually enter their “Device Advertising ID”—was highly difficult to use. The opt-out page did not provide a description of what such an ID number is or how to find it on common mobile operating systems.

Under such an implementation, a user may believe the “Device Advertising ID” is one thing (e.g., Android or iOS operating system ID, IMEI/MEID, IDFA/IFA/AAID, UDID, MAC address, etc.) when it is in fact another. Without telling a user which identifier they are to enter, the user is unlikely to know what to enter in order to opt out. And without receiving OS-specific instructions for locating their advertising ID, the ordinary user is unlikely to be able to do so. On some iOS devices, for example, in order to locate their Unique Device Identifier (UDID), a user may be required to plug his device into a computer, launch iTunes, and access precisely the correct menu screen to retrieve this ID. To obtain their iOS Identifier for Advertisers (IDFA) they would have to download and use a third-party app. Similarly, for an Android device, the user would have to manually navigate multiple menus in the built-in Settings app to locate their Advertising ID (AAID or IFA).

Furthermore, even if the user manages to select the correct ID, he must still correctly enter the 32-character alphanumeric number manually into the “Device Advertising ID” field, separated correctly by dashes, with no typographical errors. This raises a related concern: the lack of an automated verification mechanism for Kiip’s opt out.

As for the two other opt-out mechanisms that Kiip mentioned in its disclosures, our review of the disclosures yielded uncertainty about whether they applied to Kiip’s IBA or only to other entities. Providing a link to the DAA’s AppChoices app would only be beneficial to consumers looking to opt out of Kiip’s IBA if they could actually do so there. Similarly, providing users

---

<sup>37</sup> *In re: Adbrain* (72-2017), Aug. 1, 2017 at 9.

<sup>38</sup> *Id.*

with clear instructions for changing their OS-level IBA settings is a practice that is encouraged by the DAA Principles, but ambiguity as to whether or not toggling these settings will effectuate an opt out from the IBA practices of the company at issue renders them unhelpful to the end user. Providing users with choice about IBA requires giving them enough information to effectuate their decision.

Kiip's compliance solution was to update its disclosures to provide users with a link to the NAI's Mobile Choices page,<sup>39</sup> which contains clear instructions for utilizing device-level settings to opt out of IBA. Crucially, Kiip's revised disclosures describe the fact that users who follow the instructions on the NAI page will also effectuate an opt out from Kiip's IBA. By updating its notice to contain a clear description of an easy-to-use opt-out mechanism, Kiip remedied the flaws in its previous privacy disclosures—including the ambiguities about which of its enumerated opt-out methods applied to Kiip's IBA—and ensured that consumers have access to an easy-to-use opt-out mechanism. These steps resolved Kiip's compliance issues under this provision of the Mobile Guidance.

### *B. Third-party enhanced notice requirement*

Kiip acknowledged the Accountability Program's finding regarding the lack of a compliant enhanced notice link in those instances where it was collecting data through a mobile app without serving an ad.<sup>40</sup> Kiip recognized its joint obligation with first-party publishers to fulfill the enhanced notice requirement whenever personal data is collected through a mobile app for third-party IBA.

The Accountability Program's body of compliance actions has frequently focused on the provision of enhanced notice to consumers.<sup>41</sup> As we have discussed, first parties and third parties must work together to provide enhanced notice of IBA to users so they can readily access a notice about IBA that includes an opt-out mechanism.<sup>42</sup> If it is not possible for a third party to

---

<sup>39</sup> Network Advertising Initiative, *Mobile Choices, Information on Opting out on Mobile Device*, <https://www.networkadvertising.org/mobile-choice/> (last visited June 11, 2018). The Accountability Program also notes that Kiip took the further steps of updating its opt-out tool to provide users with instructions for downloading third-party apps that allow them to access their device identifiers. The company also modified its mobile ID input tool to provide users with an error message if they enter an incorrect ID. While we note that Kiip's update to its description of the NAI's Mobile Choices page would have resolved this particular compliance issue by itself, we applaud Kiip for taking additional steps to provide users the ability to exercise choice about the use of their data.

<sup>40</sup> Kiip also clarified that, in those instances where it does serve ads through a mobile app, it always provides an in-ad link to its Terms and Conditions page and an "opt out" link that appears beneath the ad container.

<sup>41</sup> See *In re: Wayfair Inc. (71-2017)*, Jan. 25, 2017 ("In practice, this first party enhanced notice link can be provided by either the first or the third party. However, both parties are independently responsible for ensuring that enhanced notice is provided. To achieve compliance, companies should work with one another to make sure that this requirement is met."). See also *In re: Exponential Interactive Inc., (73-2017)*, Aug. 1, 2017; *In re: Anheuser-Busch Companies, Inc. (70-2017)*, Jan. 25, 2017; *In re: AAA of Northern California, Nevada & Utah (69-2017)*, Jan. 25, 2017.

<sup>42</sup> See *In re: Gravity (56-2015)*, Nov. 4, 2015, at 6 ("Both first and third parties have the obligation to provide enhanced notice, and they should work together to ensure that consumers receive enhanced notice of collection or use of consumers' data for IBA. While Gravity may, as it asserts, rely on first parties' provision of enhanced notice as sufficient to fulfil its own enhanced notice obligation under the Transparency Principle, the first party's failure to

place an enhanced notice link that is accessible to consumers in a mobile app where it collects data for IBA—when, for example, it is collecting data through a non-affiliate app but not placing an ad while the app is being used—the third party must ensure that the app publisher provides an enhanced notice link as described in section III.A.(3) of the Mobile Guidance.<sup>43</sup> But whatever the circumstances, it remains the third party’s independent responsibility to ensure that this notice is provided.<sup>44</sup>

Following consultation with the Accountability Program, Kiip agreed to update its contractual documents to bind its first-party partners in the digital ad serving chain, requiring each to provide compliant enhanced notice to users as a material condition of its contract with Kiip. Kiip also committed to performing an initial assessment of its partners’ compliance with this rule. These commitments resolved Kiip’s compliance issue under the third-party cross-app enhanced notice provisions of the Mobile Guidance.

ii. Precise location data

Kiip’s collection of precise location data through the Sweatcoin application triggered the heightened requirements under the third-party precise location data provisions of the Mobile Guidance, which were crafted by industry in recognition of the sensitivity surrounding this type of data.<sup>45</sup>

A. *Third-party notice requirement*

To comply with the notice requirement of the Mobile Guidance’s precise location data provisions, Kiip updated its privacy policy to provide instructions to users about how to utilize device-level settings to withdraw consent for the collection of precise location data on an app-by-app basis. Its disclosure now also includes links to industry websites with full instructions for accessing and engaging these permissions on the Android and iOS operating systems. By providing users with clear instructions on withdrawing consent from the collection of this type of sensitive data, Kiip remedied its compliance issue under this provision of the Mobile Guidance.

B. *Third-party consent requirement*

Like other third parties in the mobile app ecosystem, Kiip did not have a direct means of communicating with users of the Sweatcoin app to obtain their consent for its collection of their precise location data. The Accountability Program has addressed this scenario before, acknowledging the technical complexities of providing consumers with the ability to consent

---

fulfill its shared responsibility to ensure that notice is provided does not excuse the third party from fulfilling its independent obligation to do so.”).

<sup>43</sup> *Mobile Guidance* at 17-18.

<sup>44</sup> *In re: MediaMath (32-2013)*, Nov. 20, 2013.

<sup>45</sup> *See 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.”).

when a company does not directly interface with them through a mobile app.<sup>46</sup> The Mobile Guidance anticipates these technological challenges and provides an alternative pathway to compliance: allowing third parties to obtain reasonable assurances from first-party app publishers that consent is obtained prior to authorizing the collection of precise location data for IBA.

To obtain reasonable assurances and comply with the third-party consent requirements of the Mobile Guidance, Kiip updated its contractual terms to ensure that its first-party partners provide their users the ability to consent to the third-party collection of precise location data for IBA. In addition, Kiip committed to incorporating an assessment of these disclosures into its routine assessment of new first-party publisher partners. Following review of Kiip's updated contractual documentation, the Accountability Program found that Kiip's terms were sufficient to serve as a compliant means of obtaining reasonable assurances from a first party, resolving this issue under the Mobile Guidance.

## **II. Compliance with the OBA Principles**

To comply with the Material Changes provision of the OBA Principles, Kiip modified its privacy disclosures to indicate to consumers that use of data that the company collects is subject to the privacy policy in effect at the time such information was first collected. On the backend, Kiip committed to adding flags to every device in its database that indicate which version of the company's privacy policy governed at the time the device entered the database. Kiip informed the Accountability Program that moving forward the company will treat data collected from each device in keeping with the terms that governed at the time of collection. These actions resolved the compliance issue under this provision of the OBA Principles.

## **III. Compliance with the Cross-Device Guidance**

During discussions with the Accountability Program, Kiip confirmed that it is engaged in cross-device IBA and acknowledged its obligations under the Cross-Device Guidance. Kiip demonstrated a clear commitment to achieving compliance with these standards. To reach compliance, Kiip updated its privacy disclosures to provide notice that the company may associate multiple devices with a particular user for IBA. The company also added language to the section of its privacy policy describing its opt-out mechanisms that indicated that opt-out choices for web browsers only apply to the specific browser where choice is exercised. The company also disclosed, consistent with the Cross-Device Guidance, that a user's mobile opt-out choice is applied on a device-specific basis. These steps provided clarity about the scope of the company's cross-device opt-out mechanisms, resolving the compliance issues under the Transparency and Consumer Control provisions of the Cross-Device Guidance.

---

<sup>46</sup> *In re: Vdopia, Inc. DBA Chocolate (85-2018)*, Aug. 20, 2018, at 10-11. See also *In re: LKQD Technologies, Inc. (77-2017)*, December 11, 2017 at 11.

## CONCLUSION

Third parties have many responsibilities under the DAA Principles, as they are generally the entities engaged in the bulk of the work associated with IBA: collecting data, sorting it, analyzing it, and using it to make intelligent decisions about serving ads to consumers. But these responsibilities are, in significant part, shared by the publisher side of the ad ecosystem. These first parties—known to consumers as brands or platforms—are often in the best position to provide certain notices, as they control the code that runs on their websites and in their apps. So, when data collection for IBA is occurring in the background of a mobile app, it is vital that first parties serve users with enhanced notice. This is especially true when sensitive data like precise location information is being collected, as consumers need to provide express consent *before* this kind of data is collected by third parties for IBA.

Accurate and complete IBA disclosures should thus be just the first step in a third party's robust approach to privacy compliance. By also making enhanced notice and, where applicable, consent standard parts of their contractual arrangements, third parties can work with first parties to make sure all consumers receive the notice and choice called for by the DAA Principles.

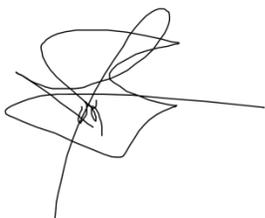
We appreciate Kiip's participation in the self-regulatory process and commend their modifications to ensure compliance with the DAA Principles.

## COMPANY'S STATEMENT

Kiip continues to be a strong supporter of the Self-Regulatory Principles for Online Behavioral Advertising, and is committed to providing transparency and maintaining best privacy practices. We appreciate the opportunity to work with the Advertising Self-Regulatory Council to continue to update our privacy disclosures to meet current industry standards.

## 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**  
**Director, Adjudications and Technology**  
**Online Interest-Based Advertising Accountability Program**