

ADVERTISING SELF-REGULATORY COUNCIL/COUNCIL OF BETTER BUSINESS BUREAUS

ONLINE INTEREST-BASED ADVERTISING ACCOUNTABILITY PROGRAM

FORMAL REVIEW
Case Number: 96-2019

COMPANY:)
IQM Corporation)
)
)
CHALLENGER:)
Online Interest-Based)
Advertising Accountability Program)
)
)

DECISION

DATE: May 22, 2019

SYNOPSIS

The Digital Advertising Alliance’s (DAA) Self-Regulatory Principles (DAA Principles)¹ cover entities engaged in interest-based advertising (IBA) across websites and mobile applications (apps). Depending on its function in a particular set of circumstances, a company can be a first party² or a third party.³ Third parties that collect multi-site data across websites must provide

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>. Unless otherwise noted, cited case names in this document refer to prior Accountability Program decisions, which may be found at <http://www.ascreviews.org/accountability-program-decisions/>.

² The term “first party” refers 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*

notice and choice to users that meet the requirements of OBA Principles. Entities engaged in IBA must also abide by the material changes provision of the OBA Principles. Third-party companies that collect cross-app data⁴ through mobile devices for IBA must provide notice and an easy-to-use opt-out mechanism to meet the requirements of the Mobile Guidance. Companies that collect precise location data through mobile apps for IBA must comply with the third-party provisions of the Mobile Guidance, including taking steps to obtain reasonable assurances of compliance from first-party partners when third parties are technologically limited from obtaining users' consent directly. The Cross-Device Guidance requires third parties 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 who own and operate websites that allow non-affiliate third parties to collect data for IBA on these websites must provide enhance notice of this fact, in compliance with the OBA Principles.

COMPANY STATUS

IQM Corporation (IQM) is an advertising technology company headquartered in New York, NY.⁵ The company specializes in political advertising.

INQUIRY

This case arises from the Accountability Program's receipt of multiple consumer complaints alleging that IQM failed to provide a functional opt-out mechanism from its collection of data for IBA. Specifically, the complaints concerned errors that consumers encountered while attempting to opt out of IQM's IBA through the DAA's WebChoices page (<http://aboutads.info/choices>) and the AppChoices app, as well as the absence of an opt-out tool on IQM's website. In each case, the consumer complained they were unable to opt out of IQM's collection of data for IBA. In light of these complaints, the Accountability Program initiated a full examination of IQM's compliance with all applicable requirements of the DAA Principles.

During its review, the Accountability Program found possible issues with IQM's compliance under the third-party provisions of the OBA Principles. Also, based on the Accountability Program's analysis of IQM's privacy disclosures, we found that IQM had possible unmet obligations as a third party under the cross-app and precise location data provisions of the

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.").

³ The term "third party" refers to entities that collect data for IBA either 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."), or from 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."). Further, the MSD Principles and Mobile Guidance together clarify that third parties are subject to the DAA Principles if they collect web viewing data across non-affiliated websites "from any type of computer or device." *Mobile Guidance* II. at 17; *MSD Principles* Definition E at 13. See IQM, *Privacy Policy* (Sept. 25, 2017), <https://iqm.com/privacy-policy> [<https://perma.cc/5CLH-PUP5>].

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.").

⁵ IQM, *Who We Are*, <https://iqm.com/who-we-are> (last visited March 20, 2019).

Mobile Guidance. Moreover, it appeared to the Accountability Program that IQM had compliance issues with the Cross-Device Guidance. Finally, the Accountability Program found possible issues with IQM’s compliance under the first-party provisions of the OBA Principles.

I. Third-party requirements review:

A. Desktop data collection for IBA review

Notice of IBA practices

The Accountability Program navigated to IQM’s privacy policy page where we found that the document described IQM’s collection and use of data for IBA as a third party. In particular, we noted language that referenced IQM’s collection of a number of data types across non-affiliate sites for the purpose of engaging in IBA in the desktop environment.⁶ However, the Accountability Program found that the disclosure lacked a statement of adherence to the DAA Principles,⁷ and we did not find a description of a mechanism to opt out of IQM’s IBA taking place on desktop devices or the mobile web.⁸

Consumer control

Looking further, the Accountability Program was unable to locate a tool for users to opt out of IBA taking place on desktop devices or through the mobile web, raising a compliance issue under the consumer control provision of the OBA Principles.

Material changes to privacy policy

The Accountability Program found that IQM’s privacy policy stated: “Use of information we collect is subject to the Privacy Policy in effect at the time such information is used.”⁹ This language indicated to the Accountability Program that consumers were subject to IQM’s then-

⁶ IQM, *Privacy Policy* (Sept. 25, 2017), <https://iqm.com/privacy-policy> (“IQM partners with numerous companies to provide online advertisements to end users of mobile websites, mobile applications (‘Apps’) and other online media (‘End Users’). As an End User browses the mobile Internet or uses Apps that include references to the IQM Service, the End User’s browser or device may request advertisements from IQM’s system. When IQM receives these requests and/or delivers advertisements to such browser or device, we may collect information about this interaction This may include, for example: IP address; ... attributes of computer or device usage, such as advertisements clicked, websites and content areas visited; browser type and version; operating system; ... and location.... The information collected under this Privacy Policy may be used to ... customize advertisements to the interests or preferences of End Users.”) [<https://perma.cc/5CLH-PUP5>].

⁷ *OBA Principles* § II.A.1. at 12 (“Such notice should include clear descriptions of the following: ... (d) The fact that the entity adheres to these Principles.”).

⁸ The Accountability Program notes that the mobile web refers to the World Wide Web users can access through their smartphones and tablets. See generally WebWise Team, *What is the mobile web?* BBC: WebWise (Oct. 10, 2012), <http://www.bbc.co.uk/webwise/guides/mobile-web>. The OBA Principles cover a company’s compliance obligations when it is engaged in IBA on the mobile web. See *In re: LKQD Technologies, Inc. (77-2017)* at 11-12, Dec. 11, 2017, <https://www.bbb.org/globalassets/local-bbbs/council-113/media/behaviorial-advertising/lkqd-decision.pdf>.

⁹ IQM, *Privacy Policy* (Sept. 25, 2017), <https://iqm.com/privacy-policy> [<https://perma.cc/5CLH-PUP5>].

effective privacy policy at the time their data is used, regardless of the version of IQM’s privacy policy that was in effect at the time their data was collected. This implied that a consumer may not be provided the opportunity to consent to material changes to IQM’s privacy policy if such changes take place between the time the user’s data is collected and the time it is used. Due to this language, the Accountability Program found a possible compliance issue under the material changes provision of the OBA Principles.

B. Mobile data collection for IBA review

i. Cross-app data collection review

Third-party notice

The Accountability Program reviewed IQM’s privacy policy to check for compliance issues related to the Mobile Guidance. During our review, the Accountability Program found that IQM’s privacy disclosures provided a description of the company’s third-party data collection for IBA taking place through mobile apps.¹⁰ While we could not locate a statement of adherence to the DAA Principles, we located a description of a mechanism to opt-out of IQM’s IBA taking place through mobile apps. The Accountability Program went on to examine this mechanism to assess its compliance with the third-party consumer control provision of the Mobile Guidance.

Third-party consumer control

Under the “Opt-Out of Interest-Based Advertising” section of its privacy policy, IQM provided instructions for users to opt out of its mobile IBA practices. For example, IQM provided the following instructions for opting out of iOS devices:

1. You can opt out of iOS distribution by providing your IDFA (Identifier for Advertising). To find your IDFA:
2. Download the app “The Identifiers app” in the App Store or another app that can display your IDFA. Please use discretion when downloading 3rd party applications.
3. **Send your IDFA to privacy@iqm.com with a request to opt-out.**¹¹

The Accountability Program found that IQM also provided opt-out instructions for Android devices. Similarly, depending on the version of Android, these instructions required users either

¹⁰ *Id.* (“IQM partners with numerous companies to provide online advertisements to end users of mobile websites, mobile applications (‘Apps’) and other online media (‘End Users’). As an End User browses the mobile Internet or uses Apps that include references to the IQM Service, the End User’s browser or device may request advertisements from IQM’s system. When IQM receives these requests and/or delivers advertisements to such browser or device, we may collect information about this interaction This may include, for example: IP address; unique identifiers sent to us from mobile devices, network carriers or data providers; information about or from the presence or use of Apps on a mobile device; The information collected under this Privacy Policy may be used to ... customize advertisements to the interests or preferences of End Users.”).

¹¹ *Id.* (emphasis added).

to download and utilize a third-party app or access their device’s settings to obtain their unique Google Advertising ID (AAID)¹² before emailing this identifier to privacy@iqm.com.

While we recognized that IQM’s disclosures included instructions to help users locate their relevant device ID, it appeared overly cumbersome to the Accountability Program that a user must manually retrieve his or her unique device identifier and send an email in order to exercise choice with respect to IBA. Therefore, we found that this implementation presented a compliance issue under the third-party cross-app consumer control provision of the Mobile Guidance.

ii. Precise location data collection review

During its review of IQM’s privacy disclosures, the Accountability Program observed language suggesting that the company may collect precise location data for IBA as a third party, raising issues under the precise location data provisions of the Mobile Guidance regarding notice and consent.¹³

C. Cross-device data collection for IBA review

The Accountability Program noted that IQM’s privacy policy appeared to indicate that the company collects and associates data across devices for IBA as a third party.¹⁴ While the Accountability Program appreciated that IQM provided language referencing its possible cross-device IBA practices, we noted some possible compliance issues. Specifically, we noted that while IQM provided a mobile opt-out mechanism, it did not explain the scope of this opt out. As discussed above, the company also did not provide an opt-out mechanism for desktop devices or for IBA taking place on the mobile web.

II. First-party requirements review

During our review, the Accountability Program observed at least one non-affiliate entity collecting data, likely for IBA, on the IQM website, which prompted us to review the company’s website for compliance with the first-party provisions of the OBA Principles.

We could not locate a description of the third-party data collection for IBA occurring on its website that would satisfy the notice requirement for first parties under the OBA Principles.

¹² See IAB Mobile Marketing Center of Excellence, Mobile Identity Guide for Marketers 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.”).

¹³ IQM, *Privacy Policy* (Sept. 25, 2017), <https://iqm.com/privacy-policy> (“We may also use the GPS location of your device if you have opted to provide it to one of IQM’s publisher or ad exchange partners. If you have questions about how to disable your device’s location services, we recommend you contact your mobile service carrier or the manufacture [sic] of your particular device.”) [<https://perma.cc/5CLH-PUP5>].

¹⁴ *Id.* (“IQM may also work with partners to collect data across browsers or devices to help predict or infer possible relationships between such browsers and devices, and such insights may be used deliver [sic] more relevant advertising across potentially related browsers and devices.”).

Further, we could not locate either a link to an industry-developed opt-out page or list of third parties with corresponding opt-out links. Finally, as described above, IQM’s disclosures did not appear to include a statement of the company’s adherence to the DAA Principles.

Moreover, in reviewing the IQM website, the Accountability Program could not locate any link that takes users **directly to** a discussion of third-party data collection for IBA **on IQM’s own website**.¹⁵ The absence of this type of link raised a compliance issue under the first-party enhanced notice provisions of the OBA Principles.

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

ISSUES RAISED

I. IQM’s obligations as a third party

A. IQM’s third-party duties under the OBA Principles

The OBA Principles govern the collection of multi-site data across websites for IBA. Third parties that engage in IBA must provide transparency (notice and enhanced notice) and consumer control (an easy-to-use opt out from IBA) when collecting or using consumers’ browsing data for IBA on non-affiliate websites.¹⁶

Notice of IBA practices

Under section II.A.(1) of the OBA Principles, a third party must provide a clear, meaningful and prominent notice of its IBA data collection and use practices, a statement of adherence to the DAA Principles, and a description of an easy-to-use mechanism for consumers to exercise choice regarding data collection for IBA.¹⁷

Consumer control

Section III.A. of the OBA Principles establishes companies’ responsibilities for providing consumers with an easy-to-use method of exercising choice with respect to the collection and use of their data for IBA.¹⁸ This choice mechanism should be available from a link in or around an advertisement, from an industry-developed consumer choice page or from a first party’s enhanced notice link.¹⁹

¹⁵ See *In re: Gravity (56-2015)*, Nov. 4, 2015, at 5 (“The enhanced notice link, which commonly is represented by the Advertising Option Icon (AdChoices Icon or Icon) and often also uses the phrase ‘AdChoices,’ should take consumers directly to the place on the third party’s own website where the third party explains its IBA activities, including the types of data collected, how it uses that data, whether it transfers the data to other, unaffiliated companies, and how the consumer can opt out of IBA from the disclosing company’s IBA practices.”).

¹⁶ *OBA Principles Summary* at 2-3. See generally *OBA Principles* §§ II.A. to III.A. at 12-14.

¹⁷ *OBA Principles* § II.A.(1) at 12.

¹⁸ *OBA Principles* § III.A. at 14.

¹⁹ *Id.*

Material changes principle

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.²⁰ 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. Consent is defined in the OBA Principles as “an individual’s action in response to a clear, meaningful, and prominent notice.”²¹

B. IQM’s third-party duties under the Mobile Guidance

i. Cross-app requirements

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.

Third-party notice

Under III.A.(1) of the Mobile Guidance, third parties must give clear, meaningful, and prominent notice of cross-app data collection for IBA. This notice must include (1) the types of data collected, (2) the uses of such data, (3) an easy to use mechanism to exercise choice with respect to data collection for IBA, and (4) a statement of adherence to the DAA Principles. This notice should be provided on a company’s website or be accessible from any app where the company is engaging in data collection for IBA.²²

Third party consumer control

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 notices required under section III.A. of the Mobile Guidance, described above.²³

ii. Precise location data requirements

Third-party notice

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

²⁰ *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.”).

²¹ *OBA Principles* Definition D at 10.

²² *Mobile Guidance* at 14-15.

²³ *Mobile Guidance* at 18-19.

precise location data to it for its use in IBA.²⁴ 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.²⁵ 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.²⁶

Third-party consent

Under section IV.B.(2) of the Mobile Guidance, a third party should obtain consent²⁷ 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.²⁸

C. IQM's third-party duties 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.²⁹

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 that explains these practices.³⁰ This notice must be posted either (1) on the company's website or (2) accessible from applications where it collects data for IBA.³¹ This notice must include a description of a choice

²⁴ *Mobile Guidance* at 22.

²⁵ *Id.* at 22-23.

²⁶ *Id.*

²⁷ *Mobile Guidance* 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.”).

²⁸ *Id.* § IV.B.(2) at 29. See the commentary to this section, which explains that third parties can meet the reasonable assurances requirement “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;” and other similar measures.

²⁹ 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.

³⁰ *Cross-Device Guidance* at 3-4.

³¹ *Id.*, n.4 (“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

mechanism for users to opt out of IBA and accurately explain the scope of the company's opt out.³²

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 provision, 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.³³ 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.³⁴ However, the Cross-Device Guidance does not require this expansive opt-out scope. 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.³⁵

II. IQM's obligations as a first party

Notice: disclosure of third-party data collection for IBA

As stated in the OBA Principles and Commentary and explicated in the Accountability Program's cases, first parties are required to provide a disclosure of the IBA activities that occur on their websites.³⁶ This disclosure must include a description of any third-party IBA activity the first party permits on its website; a statement of adherence to the DAA Principles;³⁷ and either (1) a link to an industry-developed opt-out web page such as the DAA's WebChoices page (www.aboutads.info/choices) or (2) a list of every third party engaged in IBA on the first party's website with links to each of their respective choice mechanisms.³⁸

should also indicate the Third Party's collection and use of Precise Location Data for use across devices. Consent for 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.”)

³² *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.

³³ *Id.* at 4.

³⁴ *Id.*, n.8.

³⁵ *Cross-Device Guidance* at 4 n.9.


³⁶ *OBA Principles* § II.B. at 13-14, Commentary at 32. See also *In re: Answers Corporation* (38-2014, Oct. 28, 2014), *In re: Best Buy Co.* (39-2014, Oct. 28, 2014), *In re: Yelp* (40-2014, Oct. 28, 2014), *In re: TWiT, LLC* (46-2015, May 14, 2015), and *In re: The Hollywood Reporter, Inc.* (58-2015, Jan. 14, 2016).

³⁷ If the first party's enhanced notice link, discussed below, uses the DAA's AdChoices Icon and DAA-approved wording, then it may serve independently as a site's statement of adherence to the OBA Principles.

³⁸ See *OBA Principles* §§ II.A. and II.B. at 13-14.

Enhanced notice: link to third-party IBA disclosure

In addition to the general notice requirements discussed above, first parties must ensure that an enhanced notice link is present on each webpage where a third party is collecting data for IBA purposes or serving an interest-based ad.³⁹ The enhanced notice link must take users to a page which explains the third-party IBA practices occurring on the site and provide consumers with a link to an easy-to-use opt-out mechanism. This enhanced notice link can be provided by either the website operator or a third party. However, it is the responsibility of both parties to ensure that this enhanced notice link is provided to users.

When a third party provides the enhanced notice link, generally through use of the DAA's AdChoices Icon , it may place the link either in or around the advertisement it delivers on the operator's website or, in coordination with the website operator, elsewhere on the operator's webpage. However, sometimes websites allow third parties to collect data for IBA even when no ads are being served. This appears to be the case on IQM's website. In this case, the website operator must work with third parties to allow them to provide enhanced notice or, alternatively, provide the enhanced notice itself.

If the website operator is providing the enhanced notice link, then that link should take the consumer to its own website disclosure of third-party IBA activity, discussed above. The enhanced notice link, typically provided in the footer or a sidebar on the webpage where data is being collected by any third party for IBA, must be **separate** from the link to the website's privacy policy. If the disclosure of third-party IBA activity is located in the website's privacy policy, the enhanced notice link should go **directly** to the place in the privacy policy where the disclosure is located, not just generally to the privacy policy.

COMPANY RESPONSE AND ANALYSIS

Following receipt of the Accountability Program's inquiry letter, IQM demonstrated its commitment to achieving full compliance with the DAA Principles and immediately conducted a thorough review of its data collection practices.

IQM took clear and decisive action to come into compliance, as explained below.

I. IQM's obligations as a third party

IQM's collection of multi-site data across non-affiliate websites triggered its responsibilities under the third-party provisions of the OBA Principles.

A. IQM's third-party duties under the OBA Principles

³⁹ *OBA Principles* § II.B. at 13-14.

Notice of IBA practices

To come into compliance with the notice provision of the OBA Principles, IQM updated its privacy policy to describe the scope of its data collection practices for IBA taking place in the desktop environment. It also added a statement of adherence to its privacy policy and provided a description of a new mechanism to opt out of its IBA.

Consumer control

To meet its obligations under the consumer control provisions of the OBA Principles, IQM worked with the DAA to join the industry-developed WebChoices page as a participant. IQM provided a link to WebChoices in its privacy disclosures, which resolved this issue under OBA Principles.

Material changes provision

During discussions with the Accountability Program, IQM confirmed that its business practice is not to apply material changes to its IBA activity retroactively to previously-collected data. IQM also amended its privacy disclosures to make clearer to consumers that they may be presented with choices about certain changes to the company's data collection and use practices for IBA. These actions resolved IQM's compliance issues with section V. of the OBA Principles.

B. IQM's third-party duties under the Mobile Guidance

IQM's collection of data across non-affiliate mobile apps triggered its requirements under the third-party provisions of the Mobile Guidance.

i. Cross-app requirements

Third-party notice

Under the Mobile Guidance companies must 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.⁴⁰

To achieve compliance with the third-party cross-app requirements of the Mobile Guidance, IQM took several steps. IQM updated its privacy policy to add a statement of adherence to the DAA Principles and provided a description of new mobile opt-out mechanisms, which we describe in the section below.

⁴⁰ *In re: Adbrain (72-2017)*, Aug. 1, 2017 at 9.

Third-party consumer control

The Mobile Guidance calls for companies to provide consumers with an easy-to-use choice mechanism. The Accountability Program has discussed this requirement at length in previous decisions. For example, in our decision covering LKQD Technologies, Inc., we rejected an opt-out mechanism that required that users write a letter to a company to request an opt out from the company’s IBA, finding this method incompatible with the “easy-to-use” requirement of the Mobile Guidance.⁴¹ In our *Adbrain* decision, we also found that a mobile opt-out mechanism did not meet industry standards for ease of use where that company had required users to obtain a “device ID” without any meaningful instructions about how to do so and enter it, without error, into a text entry field. Our *Adbrain* decision stated, in pertinent part:

When designing an opt-out mechanism, companies must be sure to give users access to real choice. This means that companies should make opting out easy, and they should ensure that any relevant instructions are complete, correct, and comprehensible to the typical consumer. Arcane instructions, confusing forms, and requests for information only sophisticated users or developers might know are not sufficient to assist typical consumers in opting out. In a market that is composed of consumers with a range of technical skills, an opt-out mechanism whose functionality relies on an admixture of specialized technical knowledge and trial and error on the part of its users is no opt out at all.⁴²

Similarly, in this case we raised concerns with IQM about the company’s mobile opt-out mechanism, which required users to obtain their device identifiers by utilizing a third party mobile app or access the identifier through their device’s settings, and then write an email containing this identifier to IQM requesting that the user be opted out of IQM’s IBA. During discussions with the company, we informed IQM that in our view, an opt-out mechanism that requires users to download and install a third-party application, use the application to display a unique ID, accurately copy a 32-digit string, and manually enter it—error-free—into an email message is excessively cumbersome for the average user to employ and is not “easy-to-use.”⁴³ Therefore, because we found that the barriers to effectuating IQM’s opt out were so significant, we found that the mechanism did not meet the standards set by section III.B.(1) of the Mobile Guidance, which requires that companies engaged in IBA provide consumer control to users.⁴⁴

To resolve this issue, IQM modified its privacy disclosures to provide links to clear instructions for users to access the “Opt out of interest-based ads” and “Limit Ad Tracking” operating system-level choice tools for Android and iOS devices. IQM also indicated in its disclosures that when it receives these signals for limiting ad tracking it would honor user choices. The company also worked with the DAA to integrate a cross-app mobile opt-out solution into the DAA’s AppChoices app and provided a link to this app in its updated privacy policy. These

⁴¹ See also *In re: LKQD Technologies, Inc. (77-2017)* at 3, Dec. 11, 2017, at 3-4.

⁴² *In re: Adbrain (72-2017)*, Aug. 1, 2017 at 9.

⁴³ *Id.* at 7. See also *Mobile Guidance* § III.A.(1)(c) at 14.

⁴⁴ *Mobile Guidance* at 18-19.

modifications brought IQM into full compliance with the notice and consumer control provisions of the Mobile Guidance.

ii. Precise location requirements

During discussions with the Accountability Program, IQM confirmed that it may collect precise location data for IBA through non-affiliate applications. These practices 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.⁴⁵

Third-party notice requirement

To achieve compliance with the notice provisions of precise location data requirements of the Mobile Guidance, IQM updated its privacy disclosures to include language in its privacy policy indicating that it may collect precise location data for use in IBA.⁴⁶ The company also added a new page to its website entitled “Location Privacy,” which includes instructions on the iOS and Android operating systems for disabling the collection of location data.⁴⁷ As stated above, the company also added a statement of adherence to the DAA Principles.

Third-party consent requirement

Like other third parties in the mobile app ecosystem, IQM does not have a direct means of communicating with users of first-party mobile applications to obtain their consent for the collection of precise location data. The Accountability Program has addressed this scenario before, acknowledging the technical complexities of providing consumers with the ability to consent when a company does not directly interface with them through a mobile app.⁴⁸ 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 specific consent is obtained prior to the collection of precise location data for IBA.

To obtain reasonable assurances and comply with the third-party consent requirements of the Mobile Guidance, IQM updated its contractual terms, requiring its first-party partners not to enable its collection of precise location data without first receiving users’ consent to third-party collection of precise location data for IBA. Following review of IQM’s updated contractual documentation the Accountability Program found that IQM’s terms were sufficient to serve as a

⁴⁵ 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.”).

⁴⁶ IQM, *Privacy Policy*, <https://iqm.com/privacy-policy> (last visited Sep. 28, 2018).

⁴⁷ IQM, *Location Services & Privacy*, <https://iqm.com/location-privacy> (last visited Sep. 28, 2018).

⁴⁸ *In re: Vdopia, Inc. DBA Chocolate (85-2018)*, Aug. 20, 2018, at 10-11. See also *In re: LKQD Technologies, Inc. (77-2017)*, Dec. 11, 2017, at 11.

compliant means of obtaining reasonable assurances from a first party, resolving this issue under the Mobile Guidance.

C. IQM’s third-party duties under the Cross-Device Guidance

To comply with the requirements under the Cross-Device Guidance, IQM updated its privacy disclosures to indicate 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 indicated that a user’s opt-out choice on a mobile device only applies to that device. IQM stated that it does not provide an expansive opt-out for all of a consumer’s devices and informed users that they should opt out of each of their devices to avoid the use of their data for cross-device IBA. These updates resolved the compliance issues under the Transparency and Consumer Control provisions of the Cross-Device Guidance.

II. IQM’s obligations as a first party

Notice: disclosure of third-party data collection for IBA

To come into compliance with section II.B. of the OBA Principles, IQM updates its privacy disclosures to add a page entitled “Cookie Notice” to its website. This page included a description of third-party IBA activity taking place on the IQM website, a link to the Network Advertising Initiative’s (NAI) opt-out tool, and a statement of adherence to the DAA Principles. This resolved the notice issue under the first-party provisions of the OBA Principles.

Enhanced notice: link to third-party IBA disclosure

To achieve full compliance with section II.B. of the OBA Principles, IQM added a link to its website footer, separate and apart from its privacy policy link, entitled “Cookie Notice.” This link leads users directly to the Cookie Notice page, which contains a compliant IBA disclosure at the top of the document. These implementations brought IQM into compliance with the first-party enhanced notice provisions of the OBA Principles.

CONCLUSION

The DAA Principles were intentionally designed by industry to be adaptable to new technologies and new data collection and use scenarios for IBA. Whether collecting data about a user’s browsing habits on a desktop computer or through a mobile device, or associating data across different devices, advertising technology companies must comply with the DAA Principles. In providing its wide variety of services to the marketplace, IQM touches on several distinct practices that are addressed by the evolution of the DAA Principles.

Here, IQM systematically attacked the issues raised in the Accountability Program’s letter to quickly and comprehensively reach compliance with the DAA Principles. The company implemented new consumer privacy controls, updated disclosures, and modified contractual

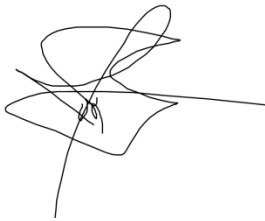
terms to address its multi-site, cross-app, precise location data, and cross-device practices. The company also added an enhanced notice link informing users about data collection occurring on the IQM site. IQM stands as a model for compliance, and the Accountability Program recognizes the diligence by which the company undertook its compliance review.

COMPANY'S STATEMENT

IQM is pleased to adopt the Self-Regulatory Principles for Online Behavioral Advertising, which are fully aligned with our commitment to transparency and consumer control. IQM appreciates the Accountability Program's thoughtful engagement to help us implement industry best practices. IQM is delighted that the Accountability Program has recognized our commitment to consumer privacy and our full compliance with the Digital Advertising Alliance's Self-Regulatory Principles.

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