ADVERTISING SELF-REGULATORY COUNCIL/COUNCIL OF BETTER BUSINESS BUREAUS

ONLINE INTEREST-BASED ADVERTISING ACCOUNTABILITY PROGRAM

FORMAL REVIEW
Case Number: 92-2019

COMPANY: Publishers Clearing House, Inc.

CHALLENGER: Online Interest-Based Advertising Accountability Program

DATE: January 28, 2019

SYNOPSIS

The Digital Advertising Alliance’s (DAA) Self-Regulatory Principles (DAA Principles)\(^1\) cover entities engaged in interest-based advertising (IBA) across websites or mobile applications (apps). Any operator of a website (a first party)\(^2\) that allows unaffiliated entities (third parties)\(^3\) to

\(^1\) The DAA’s interest-based advertising principles consist of a suite of four documents: the Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles), the Self-Regulatory Principles for Multi-Site Data (MSD Principles), the Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance) and the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (Cross-Device Guidance) (collectively, the Principles). The DAA also maintains a set of self-regulatory principles dedicated to political advertising which is not at issue in this case. The full text of the Principles can be found at http://www.aboutads.info/principles.

\(^2\) The DAA Principles assign responsibilities to an entity based on its role in a particular situation. Thus, an entity can be a first party, third party, or service provider depending on the function it is performing. Website operators are first parties. 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."). See also Online Interest-Based Advertising Accountability Program, First Party Enhanced Notice Compliance Warning CW-01-2013,
collect visitors’ web browsing data for IBA must provide visitors with notice and enhanced notice as prescribed in the OBA Principles. Additionally, mobile app publishers that authorize third parties to collect data through their apps for use in cross-app IBA must provide users with notice and enhanced notice, as described in the Mobile Guidance. Finally, if a company allows third parties to collect precise location data for IBA, it must provide users with the opportunity to consent to this collection, in addition to standard notice and enhanced notice of this fact.

COMPANY STATUS

Publishers Clearing House, Inc. (PCH) is a company that specializes in free-to-play games, contests, and sweepstakes. The company is headquartered in Jericho, New York.

INQUIRY

This case arises from consumer complaints alleging that the PCH website (http://www.pch.com/) allowed third parties to collect users’ data for use in IBA without providing enhanced notices as required by the first-party provisions of the OBA Principles. In response to these complaints, the Online Interest-Based Advertising Accountability Program (Accountability Program) reviewed the PCH website, where we observed data collection by at least 50 third-party companies known to engage in IBA. This prompted a full examination of PCH’s compliance with all applicable requirements of the DAA Principles. Below, we describe our review in detail:

I. Desktop data collection review

The Accountability Program navigated to the PCH website where we attempted to locate a compliant enhanced notice link. We located a “Privacy Policy” link in the page’s footer, which directed us to the landing page of PCH’s layered privacy policy entitled “Policy Summary.” While the language on this page referenced third-party data collection, it did not appear sufficiently clear to us to serve independently as a compliant IBA disclosure. No other link on


3 In the desktop context, third parties are entities that collect data for IBA from non-affiliate websites. See 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.”).

4 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.

5 In the mobile app context, the term “third party” refers to entities that collect data for IBA through non-affiliate mobile apps, Mobile Guidance Definition N at 12 (“An entity is a Third Party to the extent that it collects Cross-App or Precise Location Data from or through a non-Affiliate’s application, or collects Personal Directory Data from a device.”).

6 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.”).

7 For more information on the Accountability Program, and to read prior decisions referenced herein, please visit http://www.asrcreviews.org/accountability-program-decisions/.
the PCH homepage appeared to direct us to a dedicated disclosure of the third-party IBA activity occurring there.

Looking further, the Accountability Program also identified third-party advertisements that contained an AdChoices Icon being served on the PCH website. However, these were almost entirely obscured from the user’s view by an opaque JavaScript mask. This mask was placed such that users could only interact with the header and footer of the website as well as the main sweepstakes entry panel in the center of the page. The fact that users could not see or interact with these AdChoices Icons rendered them inadequate for purposes of providing consumers with enhanced notice.

The Accountability Program also observed third parties collecting IBA data on other pages of the PCH website. No third-party advertisements were visible on these pages, and we could not locate any links that would constitute enhanced notice under the DAA Principles.

Because we could not locate an enhanced notice link on PCH’s website, and because the in-ad icons we identified were effectively invisible to consumers, we believed that PCH had not met its obligations under the first-party provisions of the OBA Principles. The Accountability Program went on to review PCH’s privacy policy for a compliant IBA disclosure.

During our review, we noted that PCH’s layered privacy policy included three pages with information related to IBA: a “Policy Summary” landing page, a dedicated page labeled “Advertising,” and a page containing PCH’s full privacy policy. These pages provided progressively more complete descriptions of third-party IBA data collection and use on PCH’s website. Each of these pages also indicated that consumers could opt out from third-party ad targeting by clicking on a link leading to a TrustArc opt-out page.

Clicking on this link, the Accountability Program found that the TrustArc opt-out page listed eight companies that engage in IBA on PCH’s website along with a direct opt-out mechanism for just over half of these companies. For the remaining listed companies, the TrustArc page indicated that they had not yet been integrated to the TrustArc interface and provided links to their respective privacy policies.

The difference between the number of companies listed on the TrustArc opt-out page and the much larger number of companies that appeared to be collecting data on the PCH website raised compliance concerns. The Accountability Program noted that consumers who wished to opt out of the third-party IBA that PCH’s website enabled would only be able to opt out from a small fraction of the third parties, even if they clicked on every privacy policy linked through the TrustArc disclosure.

---

Finally, during our review of PCH’s privacy policy, we could not locate a statement of adherence to the DAA Principles.

Based on this review, we found that PCH had possible compliance issues with the OBA Principles.

II. Mobile data collection review

Following its review of the PCH website, the Accountability Program checked whether the company provided any mobile app offerings to consumers. Finding that it did, we assessed the company’s compliance with the Mobile Guidance, testing PCH’s suite of four mobile apps (The PCH App, PCH Frontpage, PCH Games, and PCH Lotto) offered on both the Android\(^\text{11}\) and iOS\(^\text{12}\) mobile operating systems.

i. Cross-app data collection review

While monitoring network traffic sent to and from both versions of The PCH App, PCH Frontpage, and PCH Lotto, the Accountability Program documented third parties known to engage in IBA collecting data through the apps. Specifically, we recorded evidence that these third parties were collecting cross-app data, including unique advertising identifiers,\(^\text{13}\) from our testing devices. The collection of this data raised issues under the first-party cross-app provisions of the Mobile Guidance.

Enhanced notice review

To assess PCH’s compliance with the mobile enhanced notice requirement, the Accountability Program first examined the privacy policy links on PCH’s mobile app listings in the Google Play Store and Apple App Store. Though some of these links directed us to the “Policy Summary” page of PCH’s privacy policy, only one of the links successfully loaded the page.\(^\text{14}\) Regardless of whether they loaded the intended page, none of these links constituted a compliant enhanced notice link under the Mobile Guidance, as they did not lead directly to a compliant disclosure of


\(^{14}\) From the Google Play Store, when we clicked on the privacy policy link for the PCH App, it directed us to a TrustArc validation page indicating that “the privacy practices of this company are not certified by TRUSTe.” This page did not contain any privacy notices for the PCH app. When we clicked on the privacy policy link for PCH Frontpage, it directed us to a 404 error page. When we clicked on the Privacy Lotto page, it directed us to the URL privacy.pch.com, but this resource did not load in our mobile web browser. From the Apple App Store, the privacy policy links loaded PCH’s Policy Summary page on the PCH App and PCH Games listings but returned a 404 error page on the Frontpage and PCH Lotto listings.
IBA taking place through PCH’s mobile apps. Though the linked Policy Summary page included some information about PCH’s IBA practices, it did not provide a description of third-party IBA activity taking place through PCH’s apps. Looking further, we could not find links to a compliant IBA disclosure either during download or upon first opening the apps, which are the alternative times at which enhanced notice may be provided.15

Looking further, the Accountability Program examined the remaining layers of PCH’s privacy policy for a compliant mobile IBA disclosure. We noted that the full policy included additional disclosures related to third-party collection of data through PCH’s apps16 as well as a description of a mechanism for users to exercise their choice to opt out of mobile IBA.17 Following the instructions in this description, we located a mobile web-based opt-out mechanism that appeared to be separate and distinct from PCH’s desktop opt-out mechanism.18

Although the instructions in PCH’s privacy policy were sufficient to engage this mobile opt out, the Accountability Program went on to test this mechanism to determine whether it resulted in a robust opt out from third-party cross-app data collection on the opted-out device.

Examining our network traffic upon first opening the mobile web-based opt-out page, the Accountability Program observed that the page received the advertising ID of our testing device. In theory, this would enable the page to substantiate the cross-app opt out. However, even after we toggled the opt-out slider on this page to the “Off” position, we continued to observe third parties known to engage in IBA collecting data through the PCH apps, including the unique advertising ID of our testing devices. These third parties included at least one company, MoPub, that is not listed on PCH’s mobile opt-out page, which continued to receive cross-app data with the parameter “DNT” flag set to “0” after the opt out was set. Our testing could not conclusively determine whether the opt out functioned for the companies that were listed on PCH’s opt-out page. Therefore, because we could not verify that PCH’s opt-out mechanism applied to the collection of cross-app data for IBA, we were concerned that PCH had a compliance issue under the enhanced notice provision of the Mobile Guidance.

---

15 The Accountability Program notes that PCH included a link to the mobile version of its TrustArc opt-out page in the settings panel for each of its mobile apps. While we commend PCH for striving to provide end users with privacy, these links did not appear in any of the required prominent locations to be compliant under the Mobile Guidance. In addition, the linked opt-out page did not constitute a fully compliant disclosure for purposes of compliance with section III.A.(3) of the Mobile Guidance.


17 Id. The Accountability Program located the following relevant disclosure:

If you are accessing our promotions and content through our mobile apps, you may opt out of such targeted advertising by opening the menu options on our APP, clicking on “Ad Preferences” and completing your opt out preferences as indicated. Please note that this will opt you out of targeted ads from PCH and any other participating advertisers. If you opt out, you will continue to receive online advertising from Publishers Clearing House; however, these ads may not be as relevant to you.

18 PCH’s mobile opt-out mechanism is also hosted by TrustArc. Unlike the opt-out page linked from the PCH.com website, this opt-out page includes a toggle switch to opt out of IBA served by “Publishers Clearing House” in addition to links to opt outs from third parties. Similar to the deficiency with PCH’s website opt out, at the time of our review the listed third parties did not represent a full list of the third parties we observed collecting data for IBA on the mobile device.
Finally, as stated in section I, PCH’s disclosures appeared to be missing a statement of adherence to the DAA Principles.

ii. Precise location data collection review

During our testing of PCH’s app offerings, the Accountability Program observed at least one third-party company that appears to be engaged in IBA collecting location information through the Android version of PCH Frontpage. The location information was in the form of latitude and longitude coordinates to the seventh decimal place, which described a point within fifteen meters of our testing device’s location.¹⁹ The Accountability Program went on to review PCH’s apps and privacy disclosures for compliance with the precise location data provisions of the Mobile Guidance.

Notice review

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

Enhanced notice review

During our review, the Accountability Program was unable to locate any enhanced notice disclosure or link that informed users about the collection of precise location data for IBA in any of the compliant times and locations prescribed by the Mobile Guidance.

User consent review

The Accountability Program noted during its review that the PCH FrontPage app used a system-default permissions dialog to request consent before it collected location data from the device. The permissions request dialog displayed the following language to users: “Allow PCH FrontPage to access this device’s location?” Users were provided the opportunity to click “Deny” or “Allow” in order to proceed. However, this dialog did not include any language disclosing that third parties would receive precise location data through the PCH FrontPage app for IBA purposes. Looking further, we could not locate any disclosure that would make clear to users that this consent mechanism would result in third-party collection of their precise location data for IBA, raising a compliance issue under the Mobile Guidance.

¹⁹ 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. 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).
Following our review, the Accountability Program sent an inquiry letter to PCH detailing these issues and explaining the requirements of the DAA Principles.

ISSUES RAISED

I. OBA Principles

First-party duties under the OBA Principles are set out in section II.B. According to this section, if first parties allow third parties to collect visitors’ browsing data for use in IBA on their websites, or if they transfer such data to third parties for tailoring ads on non-affiliate websites, they must provide consumers with appropriate transparency and an opportunity to exercise control over IBA.20 A first party must include a disclosure somewhere on its website that describes the IBA activity occurring there.21 This disclosure must contain either a link to an industry-developed consumer choice page (such as http://aboutads.info/choices) or a list of every third party conducting IBA activity on the first-party website.22 Additionally, a first party must state its adherence to the DAA Principles on its website.23

Most significantly, the OBA Principles require first parties to provide consumers with real-time “enhanced notice” when third parties are collecting or using data for IBA on a first party’s website. This real-time indicator must be in the form of a “clear, meaningful, and prominent” link that directs consumers to the first party’s IBA disclosure, not just to the top of a privacy policy.24 In addition, this link must be distinct from the company’s privacy policy link and must appear on every page where data collection or use for IBA occurs on the first party’s website. The link may be provided directly by the first party or by one of the third parties active on its website.25

Enhanced notice provides consumers with two benefits. One, the enhanced notice informs consumers of the fact that third parties are engaged in IBA on a website. Two, by linking directly to a disclosure that describes the IBA activities occurring on that website and providing a method by which consumers can exercise choice, enhanced notice serves as a bridge to relevant information consumers need at precisely the time they need it. By drawing attention to this otherwise invisible background activity in real time, explaining it in plain language, and providing one or more choice mechanisms, enhanced notice helps consumers understand IBA and make choices about the use of their data for IBA.

20 OBA Principles § II.B. at 13–14.
21 Id.
22 Id. We note that when first parties choose to list third parties individually, the Commentary to the Consumer Control Principle instructs companies that “choice should be available from the Third Party(s) disclosure linked from the page where the Third Party is individually listed.” OBA Principles Commentary at 35.
24 OBA Principles Commentary at 32 (“The Principles also state that the Web sites at which Third Parties are collecting data for Online Behavioral Advertising purposes should include a new clear, meaningful, and prominent link on their Web sites when Third Parties do not provide the notice described in II.A.2(a). This would link from the Web page where data is collected to specific language in a disclosure. If the disclosure language is in the privacy notice, the link should go directly to the relevant section of the privacy policy where the disclosure is located and not just generally to the privacy policy.”).
25 First Party Enhanced Notice Compliance Warning at 3.
II. Mobile Guidance

The Mobile Guidance adapts the desktop-oriented rules of the OBA Principles to the mobile world, including the core requirements to provide transparency and consumer control of IBA. In particular, when first parties permit third parties to collect data through their apps for use in IBA, they must provide enhanced notice and choice about such third-party data collection for IBA.26

i. First-party cross-app enhanced notice link requirement

According to section III.A.(3) of the Mobile Guidance, first parties that affirmatively authorize a third party to collect or use cross-app data for IBA must provide a clear, meaningful, and prominent link to a disclosure that (1) describes the third-party collection, (2) points to a choice mechanism/setting or lists all third parties with links to their opt outs, and (3) contains a statement of adherence to the DAA Principles.27 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.28

These enhanced notice requirements make information about privacy more accessible to users so they can make an informed decision about whether to participate in data collection and use for IBA. The enhanced notice link must go directly to the place where the app explains its IBA practices. Moreover, the link must be provided at or before the moment a user’s engagement with the app results in third-party data collection for IBA. This process provides a conspicuous, accessible and meaningful disclosure to the consumer at the time it is most useful to them. As such it is a dramatic improvement on the past practice of simply placing the information in an often dense privacy policy. It also requires that the company’s disclosure explain to consumers how they can opt out of IBA, including providing links to easy-to-use opt-out mechanisms like the DAA’s AppChoices tool.

ii. Precise location data

Notice requirement

---

26 Mobile Guidance at 17.
27 Id.
28 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 Online Interest-Based Advertising Accountability Program, Compliance Warning, http://www.asrcreviews.org/wp-content/uploads/2013/10/Accountability-Program-First-Party-Enhanced-Notice-Compliance-Warning-CW-01-2013.pdf at 2 (“Both the third party and the first party share responsibility for provision of enhanced notice. Because the third party which is collecting the data generally has no direct means to provide notice and choice on the website where its data collection is occurring, providing just-in-time notice of collection and an opt out requires cooperation between the third party engaged in the collection and the first party on whose website such collection is permitted.”).
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). 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.

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). 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. 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. Companies may use the mechanisms provided by the application store to fulfill this notice requirement. 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.

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. This consent tool should be easy to use and should apply to the application and device from which the consent is provided. The first party is also required to provide an easy-to-use tool for withdrawing consent at any time. Under the Mobile Guidance, valid consent requires an action in response to a “clear, meaningful, and prominent notice.” 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

29 Mobile Guidance at 21.
30 Id. at 21-22.
31 Id. at 23-24.
32 Id. § IV.A.(3)(b) at 24.
33 Id. See id. Commentary to § IV.A.(3) at 24 (“A First Party can satisfy the requirement to provide download notice under Section IV.A.3.a by participating in a notice mechanism that satisfies this Principle and is offered by an application platform or an application market provider that makes the application available for download.”)
34 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.
35 Id. at 23.
36 Id. at 25-26.
37 Id. § IV.B.(1)(a) at 25.
38 Id. § IV.B.(1)(b) at 26.
39 Id. § I.B. at 4.
through an application’s settings.\textsuperscript{40} A company may also use permissions tools provided by an application platform or application market provider to satisfy this requirement.\textsuperscript{41}

\textbf{COMPANY RESPONSE AND ANALYSIS}

In response to the Accountability Program’s inquiry letter, PCH immediately conducted a comprehensive review of its compliance with the DAA Principles in order to identify any areas in its compliance protocols that needed strengthening. The company provided detailed descriptions of its data collection practices, worked diligently to find comprehensive solutions to each issue, and consulted with the Accountability Program on its plan to come into compliance with the DAA Principles, as explained below.

\textbf{I. OBA Principles}

PCH’s authorization of third-party data collection for IBA on its website triggered its obligations under section II.B. of the OBA Principles to provide enhanced notice to website visitors.

The Accountability Program notes that PCH’s original implementation was partially compliant with the DAA Principles, as many companies’ implementations are. Here, PCH had availed itself of the option to provide a list of every third party engaged in IBA on its website as a pathway for compliance with section II.B. The Accountability Program acknowledges that the DAA Principles allow such a method of linking to third parties’ opt outs and that such a list may be hosted by an approved provider such as TrustArc. However, the list, whether hosted by a vendor or maintained by the first party, must be reasonably accurate. Thus, a first party that wishes to rely on an approved provider should ensure that the approved provider has access to a reasonably comprehensive list of the trackers it has authorized, for example by authorizing routine website scans.

To meet its obligations under the first-party provisions of the OBA Principles, PCH took several steps. First, the company worked with TrustArc to add a more prominent link to the DAA’s WebChoices tool to its opt-out page.\textsuperscript{42} Further, it worked with TrustArc to ensure that its opt-out page included a reasonably comprehensive list of the third-parties engaged in IBA on its website. Recognizing the difficulty in ensuring that this type of mechanism can encompass all third parties engaged in IBA on a website at all times, PCH committed to providing additional training to more of its employees. As a failsafe, PCH also invested in scanning technology to ensure that the opt-out list remains current. PCH also took steps to make sure that where TrustArc cannot supply an opt-out link for a given third party on PCH’s opt-out page, it instead provides a link to a special pop-up notification that contains links to a number of industry-developed opt-out pages, including the DAA’s WebChoices page. PCH also revised its disclosures to include a statement of adherence to the DAA Principles.

\textsuperscript{40} Id. Commentary to § IV.B.(1) at 27. The application settings may only be used by the first party to satisfy this requirement it provides notice of transfer of location data to a third party.

\textsuperscript{41} Id.

Finally, to achieve full compliance with its first-party obligations, PCH also added a link labeled “Ad Preferences” to its website footer. This link directs users to PCH’s TrustArc opt-out page.

The Accountability Program found that these steps resolved PCH’s compliance issues with the first-party enhanced notice provisions of the OBA Principles.

II. Mobile Guidance

PCH’s authorization of third-party collection of unique identifiers for IBA in its mobile app triggered compliance responsibilities under the first-party cross-app provisions of the Mobile Guidance. To meet these obligations, PCH took a number of actions.

i. Compliance with cross-app data collection requirements

The Mobile Guidance prescribes particular times and locations where consumers can receive enhanced notice that directs them to a compliant IBA disclosure. The link should appear either before or concurrent with the initial collection of data for IBA. One means for providing enhanced notice before collection occurs is to do so through a link on the app’s listing in an app store. Where possible, this can be done through a dedicated enhanced notice link, but this is not always the case. The Mobile Guidance recognizes that app stores may allow only a finite set of links dedicated to specific resources, such as company websites and privacy policies. The flexibility of the Mobile Guidance allows app publishers to use the dedicated privacy policy link as its enhanced notice link where necessary. To do so, app publishers must place an IBA disclosure or a link to a disclosure at the top of the privacy policy linked from the app store. This ensures that when a user taps on a privacy policy link in an app store listing, they are directed immediately to relevant information about IBA and an opt-out mechanism.

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

44 Mobile Guidance § III.A.(3) at 17.
45 Mobile Guidance Commentary at 18 (“Where a Third Party elects to satisfy Section III.A.2.ii.1 or a First Party elects to satisfy Section III.A.3.a by providing a link prior to installation through an application market that does not permit active links, the entity satisfies this Principle if it provides an active link to a privacy policy that contains the disclosure described in Section III.A.1 and directs consumers to the relevant section of the privacy policy where the disclosure is located.”).
To resolve its issues under the enhanced notice provisions of the Mobile Guidance, PCH updated its privacy disclosures, adding an IBA disclosure to the top of its “Policy Summary” page. This disclosure links to an updated version of PCH’s “Advertising” disclosure—which now contains a description of third-party IBA activity occurring through mobile apps—and also points users to links in the Apple App Store and Google Play Store for downloading the DAA’s AppChoices app, which can be utilized to opt out of cross-app IBA. PCH updated its Policy Summary page to include a statement of adherence to the DAA Principles. The Accountability Program found that these actions resolved PCH’s compliance issues under the first-party cross-app enhanced notice provisions of the Mobile Guidance.

**ii. Compliance with precise location data requirements**

The first DAA Principles recognized the distinction between the use of standard data types for IBA versus more sensitive data like financial or medical information. The Mobile Guidance reserved those norms of sensitivity and recognized that other, mobile-specific data types may also bear heightened scrutiny. These requirements were crafted by industry in recognition of the sensitivity surrounding these particular categories of data.

During its internal compliance review process, PCH found that it did not collect precise location data for IBA or affirmatively authorize any third party to do so. Nevertheless, PCH confirmed that third-party ad networks were collecting location data for advertising purposes without the company’s authorization. After learning of this, PCH took a number of steps to prevent third parties from accessing and using precise location data, including releasing updated versions of the PCH app that disabled the collection of location data, instituting mandatory training to employees about the precise location data provisions of the DAA Principles, and obtaining new technology to provide visibility to all apps and software development kits (SDK) to make sure that compliance issues related to privacy are identified swiftly. Weighing PCH’s responses against its own monitoring results, the Accountability Program found that these actions eliminated its concerns related to the precise location data provisions of the Mobile Guidance.

**CONCLUSION**

Today’s case continues the Accountability Program’s mission to bring mobile app and website publishers into full compliance with the DAA Principles. Popular brands that maintain consumer-facing websites and apps must provide enhanced noticed to their customers about data collection for IBA occurring on their digital properties.

---

48 OBA Principles § VI. at 16–17.
49 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.”).
Today’s case also underscores that compliance with the DDA Principles is an ongoing effort that requires companies to regularly monitor their internal operations and agreements with third parties. When a company chooses to utilize an approved service provider for a website’s opt-out mechanism, it must monitor this opt-out tool to make sure it remains up to date and free from technical errors. In addition, despite the added complexity of the mobile app space, companies must ensure that they provide notice and a functional opt-out mechanism for cross-app data collection. Crucially, when a company provides a mobile app, it should confirm whether categories of sensitive data such as a user’s precise location are being collected by third parties.

PCH demonstrated its commitment to user privacy by revising its disclosures and investing in new technologies and employee training to ensure that its desktop opt-out mechanism remains current. The company also took the laudable step of engineering a patch to its mobile app to prevent the third-party collection of precise location data for IBA.

The Accountability Program recognizes the effort that PCH expended in achieving compliance with the DDA Principles and applauds the company for its commitment to industry self-regulation and user privacy. PCH can serve as a source of emulation to other companies looking to achieve compliance with industry best practices for user privacy.

COMPANY’S STATEMENT

Publishers Clearing House is dedicated to protecting its users’ privacy. PCH has been a strong and very public supporter of DDA’s Self-Regulatory Principles since their development. In fact, PCH was one of the first publishers to endorse and be recognized for compliance with DDA Principles. PCH was also one of the leading voices among prominent brands in persuading third parties that providing consumers with notice of IBA and empowering their choice benefited the industry as well as consumers by increasing consumers’ trust. Working with the Accountability Program has been invaluable in enabling us to further enhance and build upon our established comprehensive privacy compliance program. Upon notice from the Accountability Program of the issues identified, PCH took immediate steps to address and remedy each area. Through this review process, we have implemented best-practice solutions and are pleased that such efforts have been recognized by the Accountability Program’s findings. Publishers Clearing House thanks the Accountability Office for their cooperative efforts and work that have helped us to further strengthen our longstanding commitments to the DDA Principles and protecting and enhancing our consumers’ experience.

DISPOSITION OF DECISION

Practices voluntarily corrected.
Jon M. Brescia
Director, Adjudications and Technology
Online Interest-Based Advertising Accountability Program