BakerHostetler

# Guidance on Mobile Device and Cross-App Data Collection, and Interest-Based Ads

By Alan Friel, Daniel Goldberg, and Jenna Felz

Mobile advertisers and publishers need to be aware of self-regulatory guidelines governing mobile app and device data collection and advertising practices, which became effective in September 2015. Mobile platforms such as Facebook have updated their app developer rules to require apps to comply. These rules provide for transparency (notice and enhanced notice) and choice regarding mobile data practices, including regarding the serving of so-called behavioral or interest-based advertising. This guidance document explains in detail how to comply. A simplified overview is available here: [http://www.dataprivacymonitor.com/behavioral-advertising/daa-begins-enforcing-its-guidelines-for-mobile-advertising-this-month-what-you-should-know-in-order-to-prepare/].

The United States advertising industry, which includes publishers that sell ads and those that buy and serve ads, in response to pressure from the Federal Trade Commission, created the Digital Advertising Association (DAA) for the purpose of creating a self-regulatory notice and consumer choice program for interest-based advertising (IBA). IBA is the practice of serving targeted ads to consumers based on profiles developed by tracking their behavior across time and their use of unaffiliated online services, and making inferences based on that online behavior to serve more relevant ads. IBA includes "retargeting" – the tracking of users of an online service, whether a website or a mobile app, after they leave the service, to serve them with an ad when they later visit a third-party service – a practice common for e-commerce services. The DAA also regulates collection of some types of mobile-device data for uses other than IBA, and requires notice and choice for doing so, unless the data is de-identified or its use is limited to certain operational purposes including market research and product development (Permitted Uses). It also and prohibits data collection and use for making certain sensitive eligibility determinations (e.g., credit and employment decisions). In addition, the DAA regulates collection and use of precise device location data and of data stored on a mobile device.

The DAA has issued self-regulatory principles for Online Behavioral Advertising (a/k/a IBA) [http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Full%20Text.pdf] and for Multi-Site Data [http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf] and Application of Self-Regulatory Principles to the Mobile Environment [http://www.aboutads.info/DAA_Mobile_Guidance.pdf] (DAA Principles). The DAA Principles are applied to the entire U.S. advertising ecosystem rather than being limited to a membership-based program. The DAA Principles have been in effect for years for websites, but have only recently been made effective for mobile after the DAA developed a way to overcome technical challenges inherent in the mobile environment through the development and release of a mobile app that allows consumers to register their mobile devices for opt-out. Read the description here: http://www.amazon.com/Digital-Advertising-Alliance-AppChoices/dp/B00SVQ4FMO. We explain what this means for mobile publishers and advertisers, with a focus on mobile data collection and use associated with IBA and location-aware advertising.

In short, the DAA requires a transparency (notice and enhanced-notice) and choice (opt-out) program for IBA, and has offered a uniform notice and IBA opt-out implementation tool, AdChoices (www.aboutads.info), for many years, to enable companies to comply with respect to IBA for desktop web browsing. When consumers opt out, a cookie is sent to their browser that signals Participants not to deliver IBA, and Participants look for and respond accordingly to that signal. When the DAA first looked to apply this program to mobile, there were concerns that the technology did not work for some mobile browsers and that it was incapable of being applied to mobile apps, since apps are not browser-based. Accordingly, when the DAA issued its Application of Self-Regulatory Principles to the Mobile Environment [http://www.aboutads.info/DAA_Mobile_Guidance.pdf] (Mobile Guidance) in 2013, it noted practical and technical differences between desktop computing

and mobile computing, and delayed application and enforcement until it could develop and offer Participants a similar notice and choice mechanism for mobile devices and mobile apps. That was accomplished earlier this year with the DAA's launch of two tools that enable consumers to opt out of IBA delivered to their mobile devices: AppChoices [http://www.aboutads.info/appchoices] and the DAA Consumer Choice Page for Mobile Web [http://www.aboutads.info/choices/]. These opt-out mechanisms apply to the companies listed on these choice tools, but the Mobile Guidance requires that all companies give users an easy-to-use opt-out choice either before the app is downloaded, upon download, or upon first opening of the app.

Now, as of early September 2015, the Online Interest-based Advertising Accountability Program of the Council of Better Business Bureaus' Advertising Self-Regulatory Council (Accountability Program) and the Direct Marketing Association (DMA), the organizations charged with enforcing the DAA Principles, are monitoring for violations of the Mobile Guidance.

Accordingly, mobile advertisers and publishers should look at their mobile data practices with compliance with the DAA's Mobile Guidance in mind. Notably, this will necessitate that many publishers of websites and mobile apps update their privacy notices and policies, among other things. When doing so, publishers should confirm that their privacy representations are consistent with current data practices, and make sure recently effective consumer privacy laws, such as several requirements added to California law, have been accommodated. As an example, California law now requires online services to give notice of whether third parties are collecting data via the site or app and across time and services, and if and how the publisher looks for and honors browser "do not track" signals. Compliance with, and notice of, the DAA's opt-out programs can be used to help satisfy this requirement. Advertisers should ensure that ad networks that they engage to serve IBA ads are in compliance with the DAA Principles and applicable law, and require the ad networks to ensure publishers they work with also be in compliance, including by giving the enhanced notice required by the DAA. This can be done by, for instance, adding a representation and warranty to insertion orders and purchase orders, and by making reasonable efforts to monitor for compliance.

## I. What Is the DAA's Mobile Guidance, and What Mobile Choice Tools Does It Offer?

The 2013 Mobile Guidance integrates and applies the DAA's existing Self-Regulatory Principles for Multi-Site Data [http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf] and Online Behavioral Advertising [http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Full%20Text.pdf] to the mobile environment, specifically regarding cross-app data, including its use for IBA, precise location data, and personal directory data.

### The DAA's Regulation of Mobile

The Mobile Guidance centers on the principles of **transparency** and **consumer control**, more fully explained below, in connection with the collection, use, storage, and sharing of (1) "Cross-app Data," including for IBA; (2) "Precise Location Data"; and (3) "Personal Directory Data." "Cross-app Data" is defined as "data collected from a particular device regarding application use over time and across non-affiliate applications…." "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," and "Personal Directory Data" is "calendar, address book, phone/text log, or photo/video data created by a consumer that is stored on or accessed through a mobile device." A third principle, **accountability**, is met through the DMA's and Accountability Program's monitoring and enforcement, which has now commenced.

The Mobile Guidance applies to what the DAA terms "first parties" and "third parties." A "first party" is the entity that is the app publisher, and accordingly has a direct connection with the users. A "third party" is a party that collects Cross-app Data or Precise Location Data from or through a nonaffiliate company's app, and thus has an indirect connection, or any party (including a publisher) that collects Personal Directory Data from a mobile device.

### What Are the DAA's New Choice Tools for Mobile?

The DAA Consumer Choice Page for Mobile Web [http://www.aboutads.info/choices/] is a mobile-web-optimized tool that consumers can use to opt out of the collection of cookie-based data for interest-based advertising by selected participating third parties. Similar to the desktop-optimized version, the DAA Consumer Choice Page for Mobile Web effects the opt-out by dropping a cookie on the consumer's browser that tells the applicable ad networks the consumer has opted out and should not be served IBA ads. Consumers must select which Participants they want to opt out of, and must visit the tool separately for each browser on their mobile devices (Safari, Chrome, etc.) in order for the opt-out(s) to apply to all their browsers.

Because cookie-based opt-outs do not work for mobile apps, the DAA has also released AppChoices [http://www.aboutads.info/appchoices], which is a mobile app

that allows consumers to opt out of the collection and use of Cross-app Data, other than for Permitted Uses, by listed third-party AppChoices participants (Participants). A consumer has the ability to opt out of mobile-app IBA ads from any or all of the listed Participants. Consumers may download the free mobile app from the app store available on their mobile platform (i.e., Google Play, Apple App Store, or Amazon App Store). When a consumer opts out with a particular Participant, the mobile app adds the consumer's device identifier to that Participant's opt-out list. The Participant is then notified to block the device identifiers on the opt-out list.

Both tools allow a consumer to opt out of all Participants or just selected third-party Participants. Even if a consumer opts out of all, only AppChoices Participants are notified, and non-Participants may still serve IBA, because they are not part of the program and are thus not notified. Some may offer different opt-out options, and some may be unaware of or flouting the DAA Principles. In addition, because the DAA Consumer Choice Pages for Mobile Web and AppChoices apply to separate technologies, consumers must use both to opt out of the cookie-based IBA and app-based IBA by Participants. As discussed below in Section II, these limitations of the tools could create consumer confusion if opt-out and privacy notices are not carefully worded to avoid suggesting that the tools do more than they do.

### Transparency – What Notices Are Required and by Whom?

The Mobile Guidance requires both first and third parties to give clear, meaningful, and prominent notice of their collection and use of Cross-app Data, Precise Location Data, and Personal Directory Data that are used for purposes other than the Permitted Uses of certain types of operations, system management, market research, and product development, unless the data has been de-identified. However, the constraints of mobile have resulted in notice requirements that are somewhat more relaxed than what the DAA applies to desktop browsing (see Online Behavioral Advertising [http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Full%20Text.pdf] for notice and enhanced-notice requirements for desktop browser-based IBA). Here are the mobile notice requirements:

Requirements for First Parties

- *Cross-app Data notice:* First parties must provide enhanced notice to consumers before affirmatively authorizing any third party to collect and use Cross-app Data for other than Permitted Uses, including for IBA. They must provide a clear and prominent link to a disclosure that either has a DAA-compliant choice mechanism adopted by these third parties or individually lists the third parties that will be collecting and using Cross-app Data via the app. This notice should be provided prior to, or contemporaneously with, the app's download or first use, or at the time Cross-app Data is being collected, and should also be clearly stated in the app's privacy settings or privacy policy. Notice of the AppChoices [http://www.aboutads.info/appchoices] tool is intended to satisfy this obligation as to third parties that use that tool. Accordingly, to comply with the DAA Principles, publishers should:
  - Provide notice of AppChoices [http://www.aboutads.info/appchoices] (or another compliant choice mechanism) and list any authorized third parties that do not participate in those programs, or just list all applicable authorized third parties; and
  - Indicate in the notice their adherence to the DAA Principles.

  This notice, however, is not required if the applicable third parties have obtained in-app consent from the app user prior to the collection, or have provided their own in-app notice, other than in the first party's privacy policy, that meets certain requirements including notice of an opt-out mechanism. As these are not practical options for many situations, publishers will likely find giving the enhanced notice and privacy policy notice the easiest way to comply.
- *Precise Location Data notice:* Where a first party provides Precise Location Data to a third party, or authorizes a third party to collect it, it must give clear and conspicuous notice that includes (1) the fact that Precise Location Data is transferred to or collected by a third party, (2) instructions for accessing and using a tool for providing or withdrawing consent thereto, and (3) the fact that the entity adheres to the DAA Principles. Enhanced notice of this must be given contemporaneously with the app's download or first use, or at the time of collection (which may be via a link to such notice at such time with notice also in the app's settings or privacy policy). Location-aware ads would trigger these notice requirements.

AppChoices [http://www.aboutads.info/appchoices] does not address Precise Location Data consent, so publishers will need to develop a specific choice tool or utilize one provided by the app platform or device if it can be made to function in a DAA-compliant manner.

App publishers are first parties as relates to their activities on their own and affiliated apps. However, an app publisher may also be a third party if it is collecting data from or in connection with unaffiliated apps, or collecting Personal Device Data. If so, the app will also have to comply with the notice requirements for third parties.

Requirements for Third Parties

- *Cross-app Data notice:* Third parties collecting and using Cross-app Data, other than for Permitted Uses, need to give notice of (1) the types of data collected, including any personally identifiable information; (2) the uses of such data; (3) an easy-to-use mechanism for exercising choice regarding the collection and use of such data; and (4) the fact that the entity adheres to the DAA Principles. This notice can be on the third party's website(s) or accessible from the apps from or through which they collect Cross-app Data. In addition, unless they have obtained specific consent from the app user to the collection and use, and arranged for the app to provide enhanced notice, third parties must also provide enhanced notice, which can be by participating (a) in AppChoices or another DAA-compliant opt-out tool; (b) in the first party's Cross-app Data notice as part of the download, first app use, or first Cross-app Data collection, and in the app's privacy policy, if the first party agreed to individually identify the third party in those notices or provided the third party's link to its enhanced notice as part of the download, first app use, or first Cross-app Data collection; or (c) for IBA uses only, in or around the ad.
- *Precise Location Data notice:* Third parties need to give clear, meaningful, and proximate notice of their collection and use of Precise Location Data, other than for the Permitted Uses, that explains (1) the fact that Precise Location Data is collected; (2) the use of such data (e.g., location-aware ads), including whether it will be transferred to a nonaffiliated company; (3) instructions for accessing and using the first party's tool to provide or withdraw consent to the collection and use of such data; and (4) the fact that the entity adheres to the DAA Principles. That notice should be on the third party's website(s) or accessible from the app where the data is collected, which could be by means of a link. The first party can give this notice and obtain the consent for the third party.

Advertisers buying mobile IBA or location-aware ads should make reasonable monitoring efforts to try to ensure that the ad agencies and ad networks they work with are in fact complying with all third-party obligations under the Mobile Guidance. Publishers may be held responsible not only for their own failings, but also for those of third parties they allow to interact with their services. For instance, the Accountability Program has, in the context of the required enhanced notice on browser-based IBA ads served on websites (see DAA's Online Behavioral Advertising Principles) [http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Full%20Text.pdf], brought an enforcement action against a brand that engaged ad networks to serve IBA for it, essentially holding the advertiser responsible where the third party failed to provide the on-ad notice despite the brand's claim that the ad networks had agreed to do so.

## Consumer Control: What Methods of Choice Are Sufficient?

In addition to providing notice, in certain circumstances first and third parties must obtain express consumer consent before collecting, using, and/or sharing Cross-app Data, Precise Location Data, and Personal Directory Data. However, for IBA, which is not location-aware, that choice requirement may be satisfied through an opt-out tool such as the DAA's AppChoices [http://www.aboutads.info/appchoices].

Requirements for First Parties

- *Cross-app Data notice:* First parties are required to obtain consent to their own collection and use of Cross-app Data from all or substantially all applications on a device, and provide an easy-to-use means for withdrawing consent. Third-party consent and choice compliance, including participation in a DAA-approved choice mechanism, is said by the Mobile Guidance to be the responsibility of the third party. However, the first party needs to know how that is being done for all applicable third parties in order give the correct notices in compliance with the first party's notice and enhanced-notice obligations. Further, app publishers should consider whether they are also third parties because they collect Cross-app Data from nonaffiliated apps over time. If so, they also have to comply with third-party obligations with respect to applicable nonaffiliated apps.
- *Consumer control for Precise Location Data:* First parties need to use a consumer-friendly tool to obtain consent to Precise Location Data being transferred to third parties, or for authorized third parties to collect and use such data from the first party's app, unless the third party has itself obtained that consent. This choice mechanism should also allow consumers to easily withdraw consent at any time, and the first party needs to convey that withdrawal to applicable third parties. These consents can be managed in a number of ways, including in the app's settings, so long as the enhanced-notice link directs the consumer to those settings. Providing a compliant notice of withdrawal of consent can be accomplished by uninstalling the app, if that is clearly explained in the notice. In addition, if an app publisher is receiving Precise Location Data from a nonaffiliated app, it will also need to comply with third-party obligations with respect to that other app data.
- *Consumer control for Personal Directory Data:* First parties should not affirmatively authorize any third party to intentionally access a device and obtain and use Personal Directory Data, other than for Permitted

Purposes, without express consumer authorization. App publishers are also treated as third parties, not first parties, with respect to collection of Personal Directory Data and need express consent for the collection thereof.

Requirements for Third Parties

- *Cross-app Data notice:* Only third parties are required to provide consumers with the ability to exercise choice regarding the collection and use of Cross-app Data by that third party for other than Permitted Uses. The first party's responsibility is to provide notice of that choice or facilitate that notice. Such choice should be clearly described in the notices provided to consumers, which may be given in part by the first party as described above. Participating in a DAA-approved choice mechanism such as AppChoices [http://www.aboutads.info/appchoices] is an easy way to comply, though a third party can create and manage its own choice program and mechanism. Third parties should also obtain separate express consent from consumers for Cross-app Data collection from all or substantially all apps on a consumer's device, as well as have an easy way for consumers to withdraw consent at any time.
- *Consumer control for Precise Location Data:* Third parties that collect and use Precise Location Data or transfer such data to non-affiliates for other than Permitted Uses should obtain either (1) express consumer consent for the collection, use, and transfer of the data or (2) reasonable assurances that the first party has obtained express consumer consent for the third party's receipt or collection of and use of the data, and/or its transfer to other third parties. The third party can rely on the first party for the consent withdrawal mechanism, and the first party is responsible only for conveying the withdrawal, not for the third party's ultimate honoring of the withdrawal.
- *Consumer control for Personal Directory Data:* Third parties (which here includes the app publishers) should not intentionally access a device and obtain and use personal directory data, other than for Permitted Purposes, without express consumer authorization.

## II. Tips for Compliance

- *Date of Enforcement*. With the release of the DAA Consumer Choice Page for Mobile Web and AppChoices, the DAA announced that it would begin enforcing the Mobile Guidance on September 1, 2015. Publishers, advertisers, and ad servers that have not demonstrated compliance with the Mobile Guidance risk enforcement action by the Accountability Program.
- *Ad Server vs. App Publisher and First Party vs. Third Party.* The DAA Consumer Choice Pages for Mobile Web and AppChoices are used by Participants to manage their choice obligations. Mobile app publishers should confirm with their mobile ad servers/networks what they are and are not doing to comply with the Mobile Guidance, so that they can give appropriate notice and ensure that their apps are in compliance with the DAA Principles. The Mobile Guidance purports to obligate all mobile-web and mobile-app publishers that serve IBA on their mobile sites or mobile apps to follow the DAA Principles, which essentially means publishers should not be using vendors that are not following the DAA Principles, which essentially means publishers should not be using vendors that are not following the DAA principles by either (i) participating in the two mobile tools for consumers or another DAA-approved choice program, or (ii) implementing its own choice program that meets the Mobile Guidance. Also, each app publisher should look at its own activities and determine whether it is also a third party and thus responsible for more than just first-party obligations.
- *Areas of Potential Consumer Confusion*. Various aspects of the Mobile Guidance could cause consumer confusion. One such area is the separate nature of the publisher's mobile app(s) and website(s), which might be accessed by desktop and/or mobile browsers. Consumers may not understand that mobile app opt-outs do not affect cookie-based data, while browser-based opt-outs do not affect mobile app Cross-app Data. Further, mobile app opt-outs are limited to a specific device, while browser-based opt-outs are limited to a specific browser, and that needs to be made clear to consumers. In addition, choice mechanisms are limited to the Participants of that program and the individual Participants selected for opt-out, which should also be explained. Consumers may also be confused by mobile choice mechanisms offered by other companies, such as Ghostery and TRUSTe. Unlike AppChoices, the Ghostery mobile app, at least currently, applies to the collection of cookie-based data only and not Cross-app Data. TRUSTe's mobile app, while similar to AppChoices in that it collects device identifiers from a consumer's mobile device and provides consumers the option to opt out of interest-based advertising, differs in that the opt-out extends only to third parties participating in TRUSTe's program and not necessarily to those in the DAA's program. Further, third parties can administrate their own choice programs and mechanisms. Thus, consumers may need to access multiple-choice mechanisms to completely exercise their choice with respect to a single service. Accordingly, no one opt-out will necessarily be a complete opt-out of all IBA on a publisher's sites and

apps. This should be explained in the publisher's privacy policy and in any notices or FAQs explaining the choice mechanisms, so as not to make deceptive or misleading statements about what the described choice mechanisms do and do not do. Further, it is recommended that the publisher disclaim the accuracy or reliability of third-party notices and choice mechanisms, and that its required representation of "adherence" to DAA Principles be qualified to disclaim responsibility for noncompliance by others.
Next, publishers that are both first parties and third parties need to take care in avoiding consumer confusion as to that overlap when drafting notices and privacy policy language. For instance, if a publisher also owns and operates an ad network, it is a first party as to its own apps and sites, and a third party when managing IBA across unaffiliated sites and apps for other publishers. In such a situation, the publisher, as a third-party ad network, must provide an IBA opt-out, which would not affect its status as a first party serving non-IBA ads from other IBA ad networks on that company's own apps and sites. Where the company operates under the same brand name for both its first- and third-party activities, this will not be clear to consumers and should be explained.

- *Form and Content of Notices and Privacy Policies*. The DAA's Mobile Guidance explains various ways in which its required notices are or are not effectively given. For instance, notices cannot be buried in terms and conditions. When the settings are used to provide a notice that is permissible to give there, that notice must be available in every place the settings can be accessed. Enhanced-notice links must be distinct and separate from privacy policy links. The one exception is when such notice is given in the app marketplace where the marketplace does not allow active links other than to the privacy policy. In that case, the publisher can comply if it explains exactly where in the privacy policy the user can find the enhanced-notice information by, for example, providing the precise URL. When revising privacy policies to reflect the DAA Mobile Guidance notice requirements, companies should consider doing a privacy impact assessment [http://www.dataprivacymonitor.com/cybersecurity/to-avoid-claims-assess-privacy-impacts-of-marketing-and-crm/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyMonitor+%28Data+Privacy+Monitor%29] to ensure that their privacy and data protection representations are complete and accurate. Failure to do so may cause a company's statements to be false or deceptive, and may be actionable under state and federal consumer protection laws. In addition, privacy policies may need to be updated to ensure compliance with evolving California privacy laws, which require, among other things, disclosure of third-party cross-app or cross-site tracking; how the publisher deals with "do not track" browser signals; how minors can have their publicly available posts removed from a service; and, if the operator shares personal information (broadly defined) for third-party direct marketing, how to exercise choice and control over that or receive information on which third parties were provided consumer personal information for direct marketing.
- *Technical Considerations*. Participant third parties need to be able to implement the Device ID exchange that is called for by AppChoices, and have the ability to then block IBA ads to the Device IDs on the opt-out list.

## III. Conclusion

App publishers, advertisers, and ad networks were given notice early in 2015 of the new DAA mobile consumer choice tools and the deadline for compliance with the DAA's Mobile Guidance. Parties subject to the DAA Principles, if they have followed the DAA's requirements, will have modified their privacy notices to state that they adhere to the DAA Principles. Accordingly, as of September 2015, if those companies are not fully compliant with the Mobile Guidance (as explained above), that required compliance statement will be a false representation, which may lead to an enforcement action by the Accountability Program or a claim by state and federal consumer protection agencies for deceptive commercial practices. If you have any questions, contact the Accountability Program: Genie Barton at gbarton@council.bbb.org and Jon Brescia at jbrescia@council.bbb.org. The Accountability Program is willing to help any company come into compliance outside of an enforcement action. Rather than risking a public decision noting a company's lack of compliance, companies are urged by the Accountability Program companies to take advantage of this confidential approach.

For more information, contact Alan Friel at Afriel@bakerlaw.com or 310-442-8860. Special thanks to BakerHostetler associates Daniel Goldberg and Jenna Felz for assisting the author, and to Genie Barton at the Accountability Program for providing insightful and invaluable input.