Digital Advertising Alliance

MOBILE APP IMPLEMENTATION GUIDANCE For First Parties

WHAT IS A FIRST PARTY?

Any company that owns or controls a mobile app as well as its affiliates and agents it employs.

DIGITAL ADVERTISING ALLIANCE
YourAdChoices.com AboutPoliticalAds.org PrivacyRights.info

KEYS TO CONSUMER CONFIDENCE

Transparency

You provide transparency through **enhanced notice** which alerts the consumer in real time outside of the privacy policy that unrelated companies (non-affiliates, also referred to as Third Parties) are collecting, using, or transferring data for interest-based advertising (IBA) in your mobile app. Enhanced notice should be linked directly to the place where you explain your IBA practices and how a consumer can exercise choice.

&

Consumer Control

You provide consumer control by providing access to an easy-to-use consumer choice mechanism—such as the Digital Advertising Alliance's (DAA) AppChoices app—that allows the consumer to opt out of the collection, use, or transfer of data by companies that engage in IBA. You are independently responsible for compliance, so we recommend that you follow all the steps described in this document, including always providing **enhanced notice**, notice, and access to consumer control.

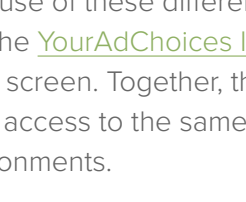
What is Interest-Based Advertising (IBA)?

Interest-based advertising (also called online behavioral advertising, tailored, or personalized advertising) is the collection of mobile app usage data, web-viewing data, precise location data, or personal directory data from a browser or device over time to serve relevant advertising based on inferences derived from such data to the consumer on unrelated apps or websites.

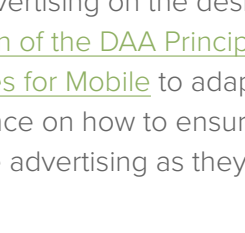
Implementing the DAA Principles in Mobile

Advertising on mobile devices is inherently different from advertising on the desktop and laptop platforms. Because of these differences, the DAA issued the Application of the DAA Principles in the Mobile Environment and the YourAdChoices Icon & Ad Marker Creative Guidelines for Mobile to adapt the Principles to the small screen. Together, these two documents provide guidance on how to ensure that mobile device users have access to the same insight into and control over mobile advertising as they already enjoy in desktop environments.

The creative guidelines provide specific, practical instructions on how to implement the mobile guidance. Through the specifications set out in the Creative Guidelines, you can use the **YourAdChoices icon** in mobile apps to give consumers the well-known visual cue (with link) to optimize the effectiveness of your enhanced notice and guide consumers to ways to exercise their choice.



Download the Application of Self-Regulatory Principles to the Mobile Environment



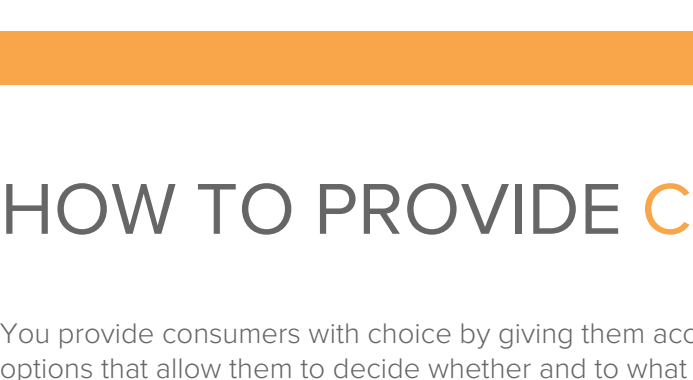
Download the YourAdChoices Icon & Ad Marker Creative Guidelines for Mobile

HOW TO PROVIDE TRANSPARENCY

Mobile App Implementation of Enhanced Notice

Provide the consumer with a clear and prominent enhanced notice link that includes the YourAdChoices icon and accompanying text such as “YourAdChoices.” Your enhanced notice link should take the consumer directly to the notice section within your privacy policy and/or any other place where you provide related disclosures.

Example of Enhanced Notice Placement & Flow



The **enhanced notice** link should be available to consumers in one or more of the following places:

- Before the app is installed, as a part of the process of downloading the app by the consumer
- When the app is opened for the first time by the consumer.
- In the app’s settings section.
- At the time IBA data is first collected by or transferred to an unrelated company for IBA.

And **notice** should include the following elements:

- A clear description of your IBA practices, including the types of data you transfer or allow unrelated companies to collect and use for IBA.
- A statement making clear that you adhere to the DAA Principles.
- An explanation of how the consumer can exercise choice.

HOW TO PROVIDE CONSUMER CONTROL

You provide consumers with choice by giving them access to at least one of the following consumer choice options that allow them to decide whether and to what extent they want to participate in IBA either by:

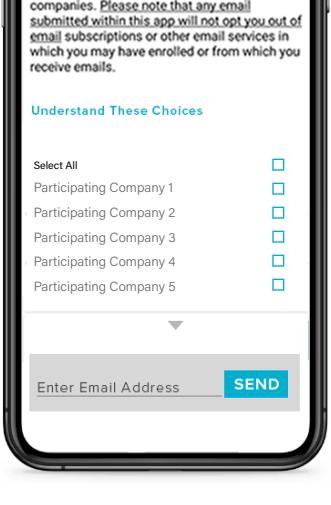
- Explaining how to use the device’s settings or operating system to exercise choice.

OR

- Listing every unrelated company collecting and using data for IBA through your app with links to their individual choice mechanisms. This list should be kept updated at all times.

OR

- Providing an explanation of and a link to download the DAA’s AppChoices tool where consumers can opt out of IBA from some or all participating companies.



When to Obtain Prior Consumer Consent

There are special requirements to obtain consent before data collection or use in these categories:

Personal Directory Data
If you access personal directory data such as a consumer’s contacts or address book, calendar, photos/videos through your app, you must obtain user authorization. You must not affirmatively authorize an unrelated company to access this data type through your app without the user’s authorization.

Precise Location Data
If you allow an unrelated company to collect precise location data for IBA, or you transfer such data to another company through your app, you should obtain a user’s consent prior to that activity and explain how to withdraw that consent.

Sensitive Health & Financial Data
You should obtain consent before you collect or transfer sensitive financial or health data to an unrelated party for use in interest-based advertising.

Data from Children Under 13
You collect data from children under 13 through your app and transfer it to an unrelated company for IBA.

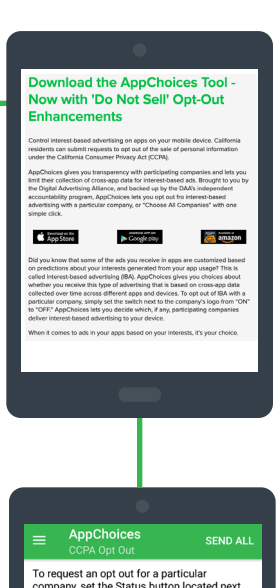
Material Change to IBA Policy & Practices
If you update your policies and practices to use previously collected data for materially different IBA purposes, you should obtain a user’s consent. Engaging in less collection or use of data for IBA is not considered a material change in practice.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA) APP GUIDANCE FOR PUBLISHERS

[The CCPA is subject to change and interpretation. The DAA is not providing legal advice or warranting that its offerings will ensure a business’s compliance with law. The guidance and use of the tools are subject to the CCPA’s requirements. All terms in this document, including “collection,” “sale,” “personal information,” “third party,” and “opt-out” are used in conformance with their definitions in the CCPA and its implementing regulations.]

There are two types of entities that collect personal information from a digital property. First, the entity that owns and operates the digital property and that collects personal information directly from a consumer (Publisher). Second, an entity that indirectly collects personal information about consumers through the publisher’s digital property (Third Party). As businesses, both Publishers and Third Parties should honor CA Do Not Sell My Personal Information requests received from California residents under the CCPA if they engage in the sale of personal information.

CA Do Not Sell My Personal Information >



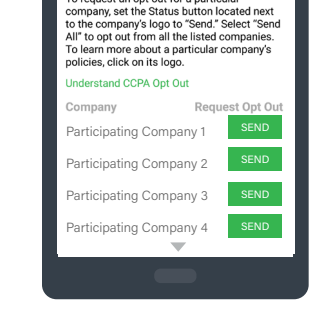
DAA’s CCPA Opt Out Tool (an enhanced version of AppChoices) for apps enables consumers to exercise their CA Do Not Sell My Personal Information rights through a consistent, recognizable system across digital properties and devices in order to express an opt out through a single location for participating entities that is effective across a participating company’s activity in apps.

The DAA’s CCPA-enhanced AppChoices for apps can be used to effectuate these requests for participating entities. When consumers make CA Do Not Sell My Personal Information requests through the tool, the entity receiving that signal should stop the sale of personal information as well as data collection used for interest-based advertising.

The DAA’s CCPA app-based tool may complement a publisher’s own opt-out tool where a consumer may have the opportunity to opt out of the sale of publisher-collected data (for example, subscriber lists, member rewards, and other covered data).

The DAA also maintains a browser-based Do Not Sell My Personal Information opt-out tool for CCPA.

Link/Notice for Third-Party Opt Out



If you are a Publisher and a Third Party collects personal information through your mobile app and sells that personal information, then you should provide an app setting that includes enhanced notice regarding the sale of information and include the Privacy Rights icon.

When clicked, this link should take consumers to a disclosure that Third Parties collect personal information through your app for advertising and analytics purposes, as well as the categories of personal information that may be collected. In this disclosure, you can also provide consumers with a link to DAA’s CCPA-enhanced AppChoices.

Example Language for Privacy Policy, App Setting or CCPA Disclosures

"Other businesses collect information when you interact with our app, including IP addresses, digital identifiers, information about your web browsing and app usage, and how you interact with our properties and ads in order to provide you with relevant ads across the Internet and for other analytics purposes, and may sell that information to other businesses for advertising and other purposes. To make opt-out requests related to mobile apps on your device for businesses participating in the DAA CCPA Opt Out tools, you can download the appropriate app at https://youradchoices.com/appchoices."

CROSS-DEVICE DATA COLLECTION FOR IBA IN MOBILE APPS

If you allow a company to collect data through your mobile app and that data is used for IBA across other devices associated with a particular browser or device, or you transfer such data to unrelated companies for this same purpose, then you should include this fact within your notice and provide a link to a choice mechanism that includes cross-device activity.

You should also direct consumers to tools that explain the scope of their choices and how they will affect their experiences online. These include the WebChoices and AppChoices tools that the DAA maintains.

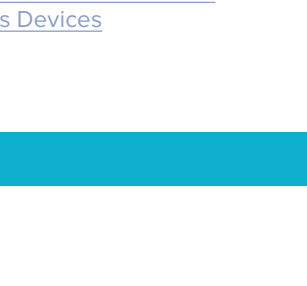
Download the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices

COMPLIANCE & ACCOUNTABILITY

The DAA Principles apply industry-wide to all companies that engage in IBA. Unlike codes that membership organizations monitor and enforce, the DAA Principles are enforced by two independent accountability programs: the BBB National Programs (BBBNP) and the Association of National Advertisers (ANA).

These programs monitor and review companies’ apps and websites throughout the
digital environment, as well as investigate consumer complaints. They bring enforcement actions against non-complying companies. The two programs publish annual reports and have released more than 125 public enforcement actions. The accountability programs also work privately with companies that seek their advice before an enforcement action to assist them confidentially to come into compliance with the DAA Principles.

We note that this document presents easy-to-follow steps that cover the basic elements of compliance with the DAA Mobile Guidance. For a more thorough review, we encourage you to read the DAA Principles and creative ad specs related to mobile. The enforcement actions and reports of the independent enforcement agents also provide advice on compliance in particular use cases. Their work is summarized in the DAA Casebook: Enforcement in Action.



Order a Free Copy

The DAA Principles apply to you as a First Party if:

- You or your affiliates own or have control over a mobile app where you authorize unrelated companies to collect data for IBA or allow unrelated companies to provide IBA on your app.
- You collect Personal Directory Data for your own use, transfer to an unrelated company, or allow an unrelated company to collect Personal Directory Data through your app for IBA.
- You collect Precise Location Data through your app and transfer it to an unrelated company or allow an unrelated company to collect Precise Location Data through your app for IBA.
- You or a Third Party collect sensitive health data, financial data, and/or data from children under 13 through your app for use in IBA.

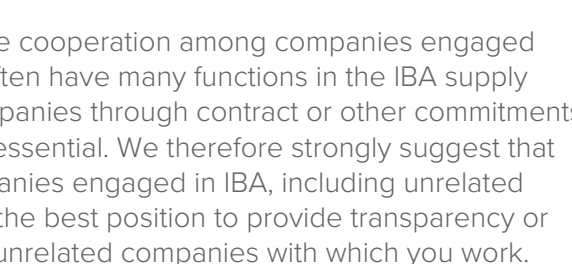
OVERVIEW OF THE DAA SELF-REGULATORY PROGRAM

The Digital Advertising Alliance (DAA) Self-Regulatory Principles are industry standards that apply to companies that engage in IBA across websites and apps. The DAA Principles establish requirements for both the publishers that operate mobile apps and websites where data is collected and the unrelated companies that collect, use, or transfer data for IBA from these sites and devices. By meeting the responsible data collection and use practices embodied in the DAA Principles, the advertising industry offers consumers innovative privacy safeguards and increases confidence in the online marketplace. These actions, in turn, preserve the ability of marketers to engage audiences with relevant advertisements, which subsidize so much of the online content and services consumers demand.

The power of the DAA Self-Regulatory Program lies in its inclusive cooperation among companies engaged in IBA throughout the digital supply chain. Because companies often have many functions in the IBA supply chain, communication, cooperation, and compliance from all companies through contract or other commitments to mutually abide by the requirements of the DAA Principles are essential. We therefore strongly suggest that you familiarize yourself with the various DAA obligations of companies engaged in IBA, including unrelated companies with which you work. As a rule of thumb, if you are in the best position to provide transparency or control about IBA, then do so on behalf of your affiliates and the unrelated companies with which you work.

IMPLEMENTING THE DAA PRINCIPLES FOR BROWSERS

When IBA is served in websites, the principles are implemented in a similar manner. The DAA has provided guidance through the Self-Regulatory Principles for Online Behavioral Advertising and Browser-Based Implementation Guidance for First Parties. Together, these documents provide guidance on how to ensure that users have insight into and control over advertising across mobile applications.



About the Digital Advertising Alliance

The Digital Advertising Alliance (DAA) is an independent not-for-profit organization which establishes and enforces responsible privacy practices for relevant digital advertising, while giving consumers information and control over the types of digital advertising they receive. The DAA manages the YourAdChoices, WebChoices, and mobile AppChoices programs. The DAA also runs the PoliticalAds program, which is designed to increase transparency and accountability around digital express advocacy ads. The DAA is managed by a consortium of the leading national advertising and marketing trade groups, including the 4A’s, American Advertising Federation, Association of National Advertisers, Interactive Advertising Bureau, and Network Advertising Initiative, along with the advice of the BBB National Programs.

Founding Associations

4A's aaf ANA BBB National Programs iab. NAI

www.digitaladvertisingalliance.org