WHAT IS A FIRST PARTY?
Any company that owns or controls a website (desktop and mobile) as well as its affiliates and agents it employs.
TRANSPARENCY & CONTROL

Transparency
You provide transparency through enhanced notice on every page of your website where unrelated parties (non-affiliates, also referred to as third parties) are collecting, using, or transferring data for interest-based advertising (IBA). Provide the consumer with a clear and prominent enhanced notice link that includes the YourAdChoices icon (     ) and accompanying text such as “AdChoices.” This 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. Enhanced notice alerts the consumer in real time outside of the privacy policy that IBA activity by non-affiliates is occurring.

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.

Consumer Control
You provide consumers with choice by giving them access to consumer choice options that allow them to decide whether and to what extent they want to participate in IBA either by:

Providing access to an easy-to-use consumer choice mechanism—such as the DAA WebChoices tool—that allows the consumer to opt out of the collection, use, or transfer of data by companies that engage in IBA and have integrated into WebChoices. This increases transparency and reduces problems associated with keeping listings up-to-date.

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

WHAT IS INTEREST-BASED ADVERTISING?
Interest-based advertising (also called online behavioral advertising, tailored, or personalized advertising) is the collection of web-viewing data, mobile app usage, precise location data, or personal directory data from a browser or device over time and across non-affiliated properties to serve relevant advertising based on inferences derived from such data to the consumer on unrelated websites or apps.
CROSS-DEVICE DATA COLLECTION

If you allow an entity to collect data through your website or app and that data is used for IBA across other devices linked to that browser or device, or you transfer such data to an unrelated party 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 may include the WebChoices and AppChoices tools that the DAA maintains.

Cross-Device Choice

CONSUMER CHOICE: OPT-OUT EXPRESSED
Third parties should not collect or transfer data from the opted-out device for IBA. And data collected from a linked device cannot be used on the opted-out device for IBA.

CONSUMER CHOICE: OPT-OUT NOT EXPRESSED
IBA data can be collected, transferred, and used among all other associated devices except those where an opt-out choice has been exercised.

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

WebChoices

www.digitaladvertisingalliance.org
© 2020 Digital Advertising Alliance. All rights reserved.
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 have released more than 100 public enforcement actions as well as publishing annual reports. 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 Principles. For a more thorough review, we encourage you to read the DAA Principles, the YourAdChoices Icon & Ad Marker Creative Guidelines, and the Mobile App Implementation Guide for First Parties. The enforcement actions and reports of the independent enforcement agents also provide advice on compliance in particular use cases. This work is conveniently summarized in the DAA Casebook: Enforcement in Action.

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

- You or your affiliates own or have control over a website where you authorize unrelated companies to collect data for IBA.
- You allow unrelated companies to provide IBA on your website.
- You collect sensitive financial or health information for your own use or transfer to an unrelated company for IBA.
- You collect data from children under 13 through your website and transfer it to an unrelated company for IBA.
CALIFORNIA CONSUMER PRIVACY ACT (CCPA)
DAA GUIDANCE FOR PUBLISHERS

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 requests received from California residents under the CCPA if they engage in the “sale” of personal information.

The DAA’s CA Do Not Sell Opt-out tool for browsers can be used to effectuate these requests for participating entities when consumers make CA Do Not Sell requests through a browser, stopping the sale of personal information. (Separately, consumers can make choices about interest-based advertising.)

The DAA’s CCPA web-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, rewards members, and other covered data).

Link/Notice for Third-Party Opt Out

If you are a Publisher and a Third Party collects personal information through your website or mobile website and sells that personal information, you should:

INCLUDE A LINK IN THE FOOTER OF YOUR WEBSITE INCLUDING THE PRIVACY RIGHTS ICON

When clicked, this link should take consumers to a disclosure that states the fact that Third Parties collect personal information through your website for advertising and analytics purposes, as well as the categories of personal information that may be collected.

EXAMPLE LANGUAGE FOR PRIVACY POLICY OR CCPA DISCLOSURES

“Other businesses collect information when you interact with our website, including IP addresses, digital identifiers, information about your web browsing activity, 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. By visiting, www.privacyrights.info or optout.privacyrights.info, you can opt out on this browser from sales of this type of personal information by businesses that participate in the opt out tool.”

The CCPA is a new and novel area, which 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.
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 and co-exist with advertising privacy laws and regulations across the globe. 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 MOBILE APPS

When IBA is served in mobile applications, the principles are implemented in similar manner. The DAA has provided guidance through the Application of Self-Regulatory Principles to the Mobile Environment and Mobile App 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.

Download the full set of DAA Self-Regulatory Principles at digitaladvertisingalliance.org/principles

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 runs the YourAdChoices 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; with the advice of the BBB National Programs (BBBNP).