Best Practices for the Application of the DAA Self-Regulatory Principles of Transparency and Control to Connected Devices

DIGITAL ADVERTISING ALLIANCE
digitaladvertisingalliance.org

JUNE 2023

DEVELOPED BY: American Association of Advertising Agencies
American Advertising Federation
Association of National Advertisers
BBB National Programs
Interactive Advertising Bureau
Network Advertising Initiative

COUNSEL: Venable LLP
Stuart P. Ingis
Michael A. Signorelli
Robert L. Hartwell

CONTENTS:

BEST PRACTICES FOR THE APPLICATION OF THE DAA SELF-REGULATORY PRINCIPLES OF TRANSPARENCY AND CONTROL TO CONNECTED DEVICES

Best Practices for the Application of the DAA Self-Regulatory Principles of Transparency and Control to Connected Devices

OVERVIEW

These best practices explain how the Digital Advertising Alliance ("DAA") Self-Regulatory Principles for Online Behavioral Advertising ("OBA Principles") and Multi-Site Data ("MSD Principles"), the Application of the Self-Regulatory Principles to the Mobile Environment ("Mobile Guidance"), and Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices ("Cross-Device Guidance") (collectively, the "Principles") apply to the practice of the collection and use of Connected Device Data from a Connected Device.

Since their inception in 2009, the DAA Principles have continued to expand and adapt to changing conditions in the ecosystem. The OBA Principles set forth guidance for data collection, use, and transfer from browsers; the Mobile Guidance addressed activity in applications on then-new mobile devices; and the Cross-Device Guidance informed the marketplace how those previous Principles can be applied to new data practices.

These best practices are intended to clarify how the principles of Transparency and Control can be applied to the collection, use, and transfer of Connected Device Data from this new class of personal consumer household devices. The DAA will build on its prior initiatives creating effective programs and implementation paths for entities engaged in covered data practices to effectuate these best practices in the marketplace.

* * *

I. Definitions

Except as defined herein, the definitions provided in the Self-Regulatory Principles and Guidance remain in full force and effect.

A. Connected Device

Connected Device means a device that connects to the Internet and is used for personal household purposes. The definition of Connected Device does not include mobile devices and web browsers to the extent that these channels are already addressed by prior DAA Principles and Guidance.

B. Connected Device Data

Connected Device Data is data about the use of a digital property or service collected from or through a Connected Device about the use of that digital property or service on a Connected Device.

> *Commentary: A "digital property" refers to the applications that operate on a Connected Device where Connected Device Data may be collected regarding a consumer's interactions with the product or service operating on the Connected Device.*

C. First Party

A First Party is the entity that controls a digital property or service that is available through a Connected Device, the entity with which the consumer intentionally interacts in order to access a digital property through a Connected Device, and its Affiliates.

> *Commentary: Agents and other entities that perform business operations for First Parties are treated as if they stand in the shoes of First Parties for purposes of these best practices.*
>
> *A consumer's intentional interactions in order to access a digital property or service through a Connected Device include, but are not limited to, where a consumer subscribes to a service like video distribution services, or where it is clear that a consumer's intentional interactions are with a portion of the digital property or service that is being operated by a different entity than the owner of the digital property or service, with the exception of any advertisements that may be served on that property or service by a Third Party. This is because it is clear that the distinct entity is the provider of the digital product or service on that portion of the digital property or service and not the operator of the initial digital property or service and that it is not a Third Party's advertisement with which the consumer is interacting. Such circumstances may arise when a video or audio player is embedded within a digital*

> *property that is clearly provided by another entity and not the First Party.*
>
> *A First Party is a Third Party to the extent that it is collecting, using, or transferring Connected Device Data from across non-Affiliate Connected Devices or services on a Connected Device and is subject to the Transparency and Control Principles applicable to Third Parties. Where a First Party instead uses a Third Party to engage in such conduct, that Third Party is subject to the Transparency and Control Principles applicable to Third Parties.*

D. Third Party

An entity is a Third Party to the extent that it collects Connected Device Data from or through a non-Affiliate's Connected Device or digital properties or services on a Connected Device.

II. Transparency

A. Third-party notice

A Third Party that collects, receives, or transfers Connected Device Data for purposes other than those enumerated in Section IV should include a disclosure within their existing notice on their own consumer-accessible digital property (e.g., website, app, etc.) that:

1. States that Connected Device Data may be:

   a. Collected, used, or transferred from or on a Connected Device;

   b. Combined with other data (including Multi-Site Data and/or Cross-App Data); and

   c. Used on Connected Devices, as well as other browsers, applications, and devices associated with the Connected Device.

2. Includes a link to a consumer choice mechanism that limits the collection, use, and transfer of Connected Device Data that meets DAA standards and applies as discussed in Section III.

3. States the fact that the entity adheres to the DAA Principles.

B. Third Party Enhanced Notice.

Third Parties should provide enhanced notice of their collection and use practices concerning Connected Device Data collected or received from a Connected Device and that links to the notice described in Section II.A. Such enhanced notice may be provided through one of the following methods, including with the cooperation of First Parties and Connected Device manufacturers where applicable:

1. In-Ad Notice where there is a visual advertisement present and users can interact with that notice, such as through a standardized QR code or interactive icon.

2. In-App Notice where a Connected Device pairs with a mobile app that can provide Enhanced Notice.

3. Device Settings where a Connected Device provides a mechanism to offer Enhanced Notice on the Connected Device.

4. Audio Notice where a Third Party collects, uses, or transfers Connected Device Data from a Connected Device through a digital property or service on a Connected Device or when a Connected Device is unable to allow a consumer to directly interact with an Enhanced Notice.

5. If there is an arrangement with the First Party for the provision of Enhanced Notice via (a) and (b),

    a. Before the application is installed, as part of the process of downloading an application to a Connected Device, at the time that the application is opened for the first time, or at the time data is collected from a Connected Device, and

    b. In the digital property or service's settings or any privacy policy.

6. Participation in a DAA-approved Choice Mechanism that individually lists participating Third Parties that is linked from the notice provided under Section II.C.

If a Third Party is unable to provide Enhanced Notice through one or more method contained in Section II.B.(1-6) above, a Third Party can provide Enhanced Notice through another method or combination of methods that provides equivalently clear, meaningful, and prominent Enhanced Notice.

C. First Party Notice

When a First Party controls a digital property or service that is available through a Connected Device and affirmatively approves a Third Party to collect and use Connected Device Data through its digital property or service, the First Party should provide a clear, meaningful, and prominent link that is reasonably accessible to a consumer in relation to how the consumer accesses the First Party's digital property or service to a disclosure hosted on the First Party's website or app that either links to an industry developed choice mechanism that provides control consistent with these best practices, or that individually lists Third Parties engaged in the collection of Connected Device Data through its digital property with links to relevant choice mechanisms. This notice should also include the fact that the entity adheres to the DAA Principles.

III. CONSUMER CONTROL

Third Parties should provide consumers with the ability to exercise choice regarding the collection and use of Connected Device Data for purposes other than those set forth in Section IV or the transfer of such data to a non-Affiliate for such purposes. Such choice should apply to the Third Party's collection, use, and transfer of Connected Device Data from which or for which the choice is exercised. Such choice mechanism should be set forth in the Enhanced Notice described in Section II.B and be available from the notice described in Section II.A, or from the Third Party's individual listing in a First Party disclosure as set forth in Section II.C.

IV. PURPOSE LIMITATIONS

Transparency and Control should be provided for Connected Device Data collected from or through a Connected Device as set forth in Sections II and III above except as follows:

(a) For operations and system management purposes, including:

(i) intellectual property protection;

(ii) compliance, public purpose and consumer safety;

(iii) authentication, verification, fraud prevention and security;

(iv) billing or product or service fulfillment, including improving customer experience or ensuring a high quality of service; or

(v) Reporting or Delivery;

(b) For Market Research or Product Development; or

(c) Where the data has or will within a reasonable period of time from collection go through a De-Identification Process.

* * *