DIGITAL ADVERTISING ALLIANCE

Powered By YourAdChoices

MAY 2019

# APPLICATION OF SELF-REGULATORY PRINCIPLES TO UNREASONABLE DATA USE PRACTICE

## OVERVIEW

This Guidance document augments the existing Self-Regulatory Principles and Guidance maintained by the Digital Advertising Alliance ("DAA"), including the Self-Regulatory Principles for Online Behavioral Advertising ("OBA"), Self-Regulatory Principles for Multi-Site Data, Application of Self-Regulatory Principles to the Mobile Environment, and Application of the DAA Principles of Transparency and Control to Data Used Across Devices. Those documents remain in full force and effect and are not limited by the following.

In this Guidance the DAA reaffirms its commitment to limiting the use of data for unreasonable purposes. Accordingly, the DAA expands the scope of its restrictions to include the use of Multi-Site, Cross-App, Precise Location, and Personal Directory Data for academic and financial aid eligibility. This important expansion is a prime example of how effective and nimble self-regulation can supplement legislative and regulatory restrictions on the use of data in an efficient manner. The DAA and its industry participants continue to evaluate what data activities are reasonable, and will update this guidance as required in the future.

When the DAA issued its first set of Self-Regulatory Principles in July 2009, it did so to provide a developing and innovative industry with a framework of reasonable and acceptable data use practices. It did so by requiring enhanced notice and control about those acceptable data practices, including the use of data for OBA. It also created independent accountability programs to monitor the ecosystem, helping companies come into compliance, and if necessary refer non-compliance to relevant government regulators.

Over the years, the DAA Principles evolved with the industry as it advanced. In 2011, industry worked through the DAA to release the Self-Regulatory Principles for Multi-Site Data. This expanded the coverage of the Principles beyond OBA, and applied the principles of Transparency and Control to all data collected from a particular computer or device regarding Web viewing over time and across non-Affiliate Web sites. The DAA also identified unreasonable uses of such data. Specifically, those Principles state that a Third Party should not collect, use, or transfer Multi-Site Data for employment, credit, and health care treatment eligibility, as well as insurance eligibility and underwriting and pricing.

With the rise of mobile devices, industry took action to address the collection of data from a particular mobile device about non-Affiliate mobile app usage over time with the Application of Self-Regulatory Principles to the Mobile Environment in 2013. The Mobile Guidance also required consent for the collection and use of Precise Location Data for certain purposes, and required authorization for the collection of Personal Directory Data. Importantly, the restrictions on certain uses of data by Third Parties were carried through to Mobile Environment guidance. While these activities were not present in the marketplace, the DAA and industry identified these uses of Multi-Site and Cross-App data as unreasonable, and worked to enforce this restriction through its independent accountability programs. This guidance provided responsive notice and control to a new platform that did not exist at the same scale when the original Principles were released in 2009, highlighting self-regulation's responsiveness and flexibility in the face of an ever changing marketplace.

In 2015, as the industry began to engage in cross-device linking to reach multi-screen consumers, DAA once again convened the industry to apply the principles of Transparency, Control, and Accountability to the practice. The Application of the DAA Principles of Transparency and Control to Data Used Across Devices quickly responded to

*(continued)*

**DEVELOPED BY:**
American Association of Advertising Agencies
American Advertising Federation
Association of National Advertisers
Council of Better Business Bureaus
Data Marketing and Analytics Division of Association of National Advertisers
Interactive Advertising Bureau
Network Advertising Initiative

**COUNSEL:** Venable LLP
Stuart P. Ingis
Michael A. Signorelli
Emilio W. Cividanes
Robert L. Hartwell

new and novel techniques in data science to provide consumers the same enhanced notice and control, and to ensure that independent accountability programs continue to help drive compliance.

The DAA's privacy principles and guidance serve as one of the nation's leading examples of how self-regulatory bodies can work within a statutory framework to enhance consumer privacy and data security protections. The restrictions provided here continue the decades-plus effort of the digital advertising industry to evaluate its practices and restrict its participants from engaging in unreasonable uses of data. The DAA's effort will continue as the industry and technology innovates and grows.

## I. Definitions

**A. Affiliate**
An Affiliate is an entity that Controls, is Controlled by, or under common Control with, another entity.

**B. Control**
Control of an entity means that one entity (1) is under significant common ownership or operational control of the other entity, or (2) has the power to exercise a controlling influence over the management or policies of the other entity. In addition, for an entity to be under the Control of another entity and thus be treated as a First Party under these Principles, the entity must adhere to policies with respect to Multi-Site Data, Cross-App Data, Precise Location Data, and Personal Directory Data that are not materially inconsistent with the other entity's policies.

**C. Cross-App Data**
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.

**D. First Party**
A First Party is the entity that is the owner of a Web site or an application, or has Control over the Web site or application, with which the consumer interacts, and its Affiliates.

**E. Multi-Site Data**
Multi-Site Data is data collected from a particular computer or device regarding Web viewing over time and across non-Affiliated Web sites.

**F. Personal Directory Data**
Personal Directory Data is calendar, address book, phone/text log, or photo/video data created by a consumer that is stored on or access through a particular device.

**G. Precise Location Data**
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.

**H. Third Party**
An entity is a Third Party to the extent that it collects Multi-Site Data, Cross-App Data, or Precise Location Data from or through a non-Affiliate's Web site and/or application, or collects Personal Directory Data from a device.

## II. Restrictions on the Use of Multi-site Data for Eligibility for Employment, Credit, Health Care, Insurance or Education

Notwithstanding any other provisions, Multi-Site Data, Cross-App Data, Precise Location Data, and Personal Directory Data should not be collected, used, or transferred for the following purposes:

**A. Employment Eligibility**
Determining adverse terms and conditions of or ineligibility for employment, promotions, reassignment, sanction, or retention as an employee.

**B. Credit Eligibility**
Determining adverse terms and conditions of or ineligibility of an individual for credit.

**C. Health Care Treatment Eligibility**
Determining adverse terms and conditions for or ineligibility of an individual to receive health care treatment.

**D. Insurance Eligibility and Underwriting and Pricing**
Determining adverse terms and conditions of or ineligibility of an individual for insurance, including, but not limited to, health insurance.

**E. Education Eligibility**
Determining adverse terms and conditions of or ineligibility for admission, sanction, or retention as a student.

*Commentary: An entity would not be in violation of this provision if the entity transfers such data with the reasonable basis for believing it will be used for purposes enumerated in III. A-C, and the recipient then misuses the data for a purpose that is prohibited by this provision.*

## III. Purpose Limitations

Transparency and control should be provided for Multi-Site Data, Cross-App Data, Precise Location Data, and Personal Directory Data as set forth in the Principles 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.

*Commentary: Data collected for a purpose listed in Section III should not be used for a purpose other than those listed in Section III without providing transparency and control as described in the Principles.*

* * *