Application of Self-Regulatory Principles to the Mobile Environment

DIGITAL ADVERTISING ALLIANCE

www.AboutAds.info

JULY 2013

DEVELOPED BY: American Association of Advertising Agencies
American Advertising Federation
Association of National Advertisers
Council of Better Business Bureaus
Direct Marketing Association
Interactive Advertising Bureau
Network Advertising Initiative

COUNSEL: Venable LLP
Stuart P. Ingis
Emilio W. Cividanes
Michael A. Signorelli
Julia Kernochan Tama

CONTENTS

APPLICATION OF SELF-REGULATORY PRINCIPLES TO THE MOBILE ENVIRONMENT

Application of Self-Regulatory Principles to the Mobile Environment

OVERVIEW

This guidance explains for covered companies how the existing Digital Advertising Alliance ("DAA") Self-Regulatory Principles for Online Behavioral Advertising ("OBA Principles") and Multi-Site Data ("MSD Principles") (collectively, the "Self-Regulatory Principles") apply to certain types of data in the mobile Web site and application environment. This guidance responds to the fact that both First Parties and Third Parties operate across a variety of channels including mobile. The Self-Regulatory Principles apply consistently across these channels, although current implementation may vary based on the technological demands of different channels.

The existing Self-Regulatory Principles and definitions remain in full force and effect, including the purpose limitations set forth in the MSD Principles, and the commentary for such Principles also applies in the mobile Web site and application environment where relevant. For clarity and ease of use, this guidance document restates many of the standards and definitions from the OBA Principles and MSD Principles. These definitions should be

interpreted consistently across channels. In the future, the DAA intends to release a consolidated set of Self-Regulatory Principles that integrates this guidance document with the OBA Principles and MSD Principles, resulting in one uniform set of Principles.

Section II of this guidance clarifies that the previously-issued Self-Regulatory Principles apply to the mobile Web site environment. Due to the technical features of different types of devices and systems, the DAA recognizes that it may not be feasible to comply with the Self-Regulatory Principles on the mobile Web in the same manner as in a desktop computer environment. From time to time, the DAA may provide guidance on implementation practices.

Sections III, IV, and V of this guidance explain how the Self-Regulatory Principles apply to certain data practices that may occur on mobile or other devices. Section III sets forth how the Principles apply to data collected from a particular device regarding application use over time and across non-Affiliate applications. Section IV explains the application of the Principles to Precise Location Data – data obtained from a device about the physical location of the device that is sufficiently precise to locate a specific individual or device. Entities subject to this guidance can use multiple existing technologies to satisfy this section. Section V addresses Personal Directory Data – calendar, address book, phone/text log,

or photo/video data created by a consumer that is stored on or accessed through a device.

The DAA will build on the success of its existing Web-based uniform choice mechanism by working with DAA stakeholders to develop and implement, or otherwise specify, a companion choice mechanism or setting for Cross-App Data. During this implementation phase, this guidance with respect to Cross-App Data, Precise Location Data, and Personal Directory Data will not be in effect or enforced by the DAA accountability mechanisms. After such choice mechanism is operational and the DAA has announced to covered companies that this guidance is effective and enforceable, any entity engaged in the collection and use of Cross-App Data, Precise Location Data, or Personal Directory Data after the effective date established by the DAA will be subject to the DAA accountability mechanisms for engaging in practices that do not adhere to the Self-Regulatory Principles as clarified in this guidance.

I. DEFINITIONS

A. Affiliate

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

B. Consent

Consent means an individual's action in response to a clear, meaningful, and prominent notice regarding the collection and use of data for a specific purpose. Where an entity has a relationship with a consumer through an additional or different medium than the device to which Consent applies, Consent may be obtained through any such medium.

> *Commentary: Pursuant to this definition, an entity may obtain Consent through a device other than the device to which the Consent applies. For example, where an entity offers a video viewing service that is available to subscribers on non-mobile devices and is also available on mobile devices, the entity may obtain Consent through a non-mobile device that applies to one or more mobile devices.*

C. 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 con-

trolling 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 Cross-App Data, Precise Location Data, and Personal Directory Data that are not materially inconsistent with the other entity's policies.

D. 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.

> *Commentary: Cross-App Data includes unique values assigned or attributed to a device or a unique combination of characteristics associated with a device where combined with Cross-App Data. Cross-App Data does not include data that is not associated with a specific individual or device, such as data that has been De-Identified.*
>
> *Cross-App Data does not include data that is collected about non-Affiliate applications but is not associated or combined across such applications. If a Third Party associates or combines previously-collected data to create Cross-App Data, the obligations under these Principles are triggered at the time that the entity creates such Cross-App Data.*

E. De-Identification Process

Data has been De-Identified when an entity has taken reasonable steps to ensure that the data cannot reasonably be re-associated or connected to an individual or be connected to or associated with a particular computer or device.

An entity should take reasonable steps to protect the non-identifiable nature of data if it is distributed to non-Affiliates and obtain satisfactory written assurance that such entities will not attempt to reconstruct the data in a way such that an individual may be re-identified and will use or disclose the de-identified data only for uses as specified by the entity.

An entity should also take reasonable steps to ensure that any non-Affiliate that receives de-identified data will itself ensure that any further non-Affiliate entities to which such data is disclosed agree to restrictions and conditions set forth in this subsection I.E.

F. Delivery

Delivery is the delivery of online content, advertisements, or advertising-related services using Reporting data. Delivery does not include the collection and use of Reporting data when such data is used to deliver online advertisements or advertising-related services to a computer or device based on the preferences or interests inferred from information collected over time and across non-Affiliate

mobile Web sites because this type of collection and use is covered by the definition of Online Behavioral Advertising in the Self-Regulatory Principles for Online Behavioral Advertising.

G. First Party

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

> *Commentary: Agents and other entities that perform business operations of First Parties are treated as if they stand in the shoes of First Parties under these Principles. Similarly, this traditional legal construct of agents would apply to Third Parties and their agents and other entities that perform business operations of Third Parties. If an agent is taking on the responsibility of an entity that is a First Party or Third Party, either the agent or that entity would have to satisfy the obligations under these Principles. Thus, an entity cannot escape its obligations by outsourcing its responsibilities to an agent.*

H. Market Research

Market Research means the analysis of: market segmentation or trends; consumer preferences and behaviors; research about consumers, products, or services; or the effectiveness of marketing or advertising. A key charac-

teristic of market research is that the data is not re-identified to market directly back to, or otherwise re-contact a specific computer or device. Thus, the term "market research" does not include sales, promotional, or marketing activities directed at a specific computer or device.

> *Commentary: Any contact back to a computer or device that is based on an aggregate use of data that may have been collected from such computer or device is not disqualified from being "market research" because data collected from such computer or device was included in the aggregate use.*

I. 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 accessed through a particular device.

> *Commentary: Personal Directory Data includes unique values assigned or attributed to a device or a unique combination of characteristics associated with a device where combined with Personal Directory Data. Personal Directory Data does not include data that is not associated with a specific individual or device, such as data that has been De-Identified.*

J. Personally Identifiable Information ("PII")

Personally Identifiable Information is information about a specific individual including name, address, telephone number, and email address – when used to identify a particular individual.

K. 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.

> *Commentary: Precise Location Data includes unique values assigned or attributed to a device or a unique combination of characteristics associated with a device where combined with Precise Location Data. Precise Location Data does not include data that is not associated with a specific individual or device, such as data that has been De-Identified.*
>
> *Precise Location Data does not include location data that is not precise, including location data that has been or will be rendered not precise within a reasonable period of time from collection and during that period of time is not used for purposes other than those set forth in Section VI. Precise Location Data may include, for example, data obtained from cell tower or Wi-Fi triangulation techniques, or latitude-longitude coordinates obtained through GPS technology, if*

such data is sufficiently precise to locate a specific individual or device. Precise Location Data does not include five-digit ZIP code, city name, general geographic information whether derived from an IP address or other sources, or information that does not necessarily reflect the actual location of a device such as information entered by a user or a billing address associated with an account.

Due to the technical limitations of different types of devices and systems, the DAA recognizes that it may not be feasible to comply with this guidance regarding Precise Location Data on all devices in the same manner. From time to time, the DAA may provide guidance on implementation practices for compliance with the Self-Regulatory Principles across different types of devices and systems.

L. Product Development

Product Development means the analysis of: (1) the characteristics of a market or group of consumers; or (2) the performance of a product, service or feature, in order to improve existing products or services or to develop new products or services. Like data used for Market Research, data used for Product Development is not re-identified to market directly back to, or otherwise re-contact a specific computer or device.

> *Commentary: Any contact back to a computer or device that is based on an aggregate use of data that may have been collected from such computer or device is not disqualified from being "product development" because data collected from such computer or device was included in the aggregate use.*

M. Reporting

Reporting is the logging of Cross-App Data, Precise Location Data, or Personal Directory Data on an application or the collection or use of other information about an application, operating system, date and time of viewing of the application or advertisement, or impression information for:

- Statistical reporting in connection with the activity on an application;
- Analytics;
- Optimization of location of ad and media placement;
- Reach and frequency metrics (*e.g.,* frequency capping);
- Ad performance; and
- Logging the number and type of advertisements served on a particular application.

N. Third Party

An entity is a Third Party to the extent that it collects Cross-App Data or Precise Location Data from or through a non-Affiliate's application, or collects Personal Directory Data from a device.

> *Commentary: An entity may be a Third Party with respect to some of its activities or services, and not for its other activities or services. An entity may be a Third Party if it collects Cross-App Data, Precise Location Data, or Personal Directory Data by providing software development kits or other technical tools that are integrated into a non-Affiliate's application.*
>
> *In addition, in certain situations where it is clear that the consumer is interacting with a portion of an application that is not an advertisement and is being operated by a different entity than the owner of the application, the different entity would not be a Third Party for purposes of the Principles, because the consumer would reasonably understand the nature of the direct interaction with that entity. The situation where this occurs most frequently today is where an entity through a "widget" or "video player" enables content and it is clear that such content is not an advertisement and that portion of the application is provided by the other entity and not the First Party application. The other entity (e.g., the "widget" or "video player") is directly interacting with the consumer and, from the consumer's perspective, acting as a First*

Party. Thus, it is unnecessary to apply to these activities the Principles governing data collection and use by Third Parties with which the consumer is not directly interacting.

II. TRANSPARENCY AND CONTROL FOR MULTI-SITE DATA

The collection and use of Multi-Site Data from any type of computer or device is covered by the Self-Regulatory Principles for Multi-Site Data.

Commentary: Mobile devices may be used to access Web sites. Due to the technical limitations of different types of devices and systems, however, the DAA recognizes that it may not be feasible to comply with the Self-Regulatory Principles on all devices in the same manner as in a desktop computer environment. From time to time, the DAA may provide guidance on implementation practices for compliance with the Self-Regulatory Principles across different types of devices and systems.

The DAA recognizes, for example, that on devices with small screens it may not be feasible to provide notice of Multi-Site Data collection on the specific Web page where such data is collected even if there is an arrangement with the First Party for the provision of such notice. In such cases, it is acceptable for notice to be provided where such notice is clear, meaningful, and prominent.

III. TRANSPARENCY AND CONTROL FOR CROSS-APP DATA

A. TRANSPARENCY

1. Third Party Notice

Third Parties should give clear, meaningful, and prominent notice of their Cross-App Data collection and use practices for purposes other than those set forth in Section VI. Such notice should include clear descriptions of the following:

(a) The types of data collected, including any Personally Identifiable Information;
(b) The uses of such data, including whether it will be transferred to a non-Affiliate;
(c) An easy-to-use mechanism for exercising choice with respect to the collection and use of such data or the transfer of such data to a non-Affiliate for purposes other than those set forth in Section VI; and
(d) The fact that the entity adheres to these Principles.

Third Parties should provide such notice on their own Web sites or accessible from any application from or through which they collect Cross-App Data.

2. Third Party Enhanced Notice on Cross-App Data

In addition to providing notice as described in Section III.A.1, Third Parties should provide enhanced

notice of their Cross-App Data collection and use practices for purposes other than those set forth in Section VI. Such enhanced notice should be provided as set forth below in (a) or (b):

(a) Application Notice: Third Parties should provide notice through a clear, meaningful, and prominent link to a disclosure described in Section III.A.1 that is presented within the application as follows:
    (i) In or around an advertisement delivered using Cross-App Data or
    (ii) If there is an arrangement with the First Party for the provision of such notice,
        1. Before the application is installed, as part of the process of downloading an application to a device, at the time that the application is opened for the first time, or at the time Cross-App Data is collected, and
        2. In the application's settings or any privacy policy.

(b) Participation in Choice Mechanism(s) or Setting(s): Third Parties that do not provide enhanced notice through one of the methods set forth in subparagraph (a) should be individually listed either:

(i) On a mechanism or setting that meets Digital Advertising Alliance specifications and is linked from the disclosure described in Section III.A.3 or

(ii) If agreed to by the First Party, in the disclosure described in Section III.A.3.

Third Parties that obtain Consent prior to collecting or using Cross-App Data for purposes other than those set forth in Section VI are not subject to this Third Party Enhanced Notice Principle.

> *Commentary: When notice is provided in application settings under these Principles, such notice should be available from each location where settings are available. When notice is provided in an application privacy policy, such policy may be provided within the application or may be provided on a mobile-optimized website that is linked from the application.*
>
> *Any requirement in this guidance to provide clear, meaningful, and prominent notice would not be satisfied by providing notice hidden in lengthy terms and conditions. Similarly, if enhanced notice is provided through the method set forth in Section III.A.2.a.ii, the link provided under Section III.A.2.a.ii.1 must be distinct from the First Party's link to its privacy policy. For example, this require-*

> *ment to provide a clear, meaningful, and prominent link to a disclosure could be satisfied with a new link to specific language within a disclosure.*

3. First Party Enhanced Notice

When First Parties affirmatively authorize any Third Party to collect and use Cross-App Data for purposes other than those set forth in Section VI, the First Party should provide a clear, meaningful, and prominent link to a disclosure that either points to a choice mechanism or setting that meets Digital Advertising Alliance specifications or individually lists such Third Parties. Such link should be provided:

(a) Before the application is installed, as part of the process of downloading an application to a device, at the time that the application is opened for the first time, or at the time Cross-App Data is collected, and
(b) In the application's settings or any privacy policy.

A First Party should indicate adherence to these Principles in such disclosure. A First Party does not need to provide a link to such disclosure in instances where the Third Party provides notice as described in Section III.A.2.a above or obtains Consent prior to collecting or using Cross-App Data for purposes other than those set forth in Section VI.

Commentary: A First Party is only subject to this Principle when it has affirmatively authorized the Third Party to collect the data. For the purpose of this Principle, in instances where a Third Party may be collecting data from a First Party, where the First Party has not affirmatively authorized such collection, there is not an obligation on the First Party to provide notice of such collection.

Where a Third Party elects to satisfy Section III.A.2.ii.1 or a First Party elects to satisfy Section III.A.3.a by providing a link prior to installation through an application market that does not permit active links, the entity satisfies this Principle if it provides an active link to a privacy policy that contains the disclosure described in Section III.A.1 and directs consumers to the relevant section of the privacy policy where the disclosure is located.

B. CONSUMER CONTROL

1. Third Party Choice

Third Parties should provide consumers with the ability to exercise choice regarding their collection and use of Cross-App Data for purposes other than those set forth in Section VI or the transfer of such data to a non-Affiliate for such purposes. Such choice should apply to the Third Party's collection

and use of Cross-App Data from the device from which or for which the choice is exercised. Such choice should be described in the enhanced notice described in Section III.A.2.a or should be available from the choice mechanism described in Section III.A.2.b.i or from the Third Party's individual listing in a First Party disclosure as set forth in Section III.A.3.

> *Commentary: A Third Party that provides consumers access to a mechanism or setting offered by a platform or operating system that provides the ability to exercise choice consistent with this Principle satisfies this Principle. Choice under this Principle applies to future data collection, use, and transfer for purposes other than those set forth in Section VI.*

2. Consent for Cross-App Data Collection from All or Substantially All Applications

   (a) Consent: Entities should not collect and use Cross-App Data through such entities' provision of a service or technology that collects Cross-App Data from all or substantially all applications on a device, for purposes other than those set forth in Section VI, without Consent. Such Consent should apply to the device from which or for which the Consent is provided.

(b) Withdrawing Consent: Entities that have obtained Consent for collection and use of such data for such purposes should provide an easy-to-use means to withdraw such Consent.

Commentary: Section III.B.2 applies to an entity's service or technology that collects all or substantially all Cross-App Data regardless of the specific applications installed on a device, and not to its other services or technologies. This standard is not specific to any particular type of service or technology.

Consent or a withdrawal of Consent under this Principle applies to future data collection, use, and transfer for purposes other than those set forth in Section VI. An entity that directs consumers to their device or platform settings, if such settings allow consumers to provide or withdraw Consent for the collection and use of Cross-App Data with respect to a specific device, satisfies this Principle. As described in the definition of "Consent," where an entity has a relationship with a consumer through an additional or different medium than the device to which Consent applies, Consent may be obtained through any such medium.

IV. TRANSPARENCY AND CONTROL FOR PRECISE LOCATION DATA

A. TRANSPARENCY

1. First Party Notice

First Parties should give clear, meaningful, and prominent notice of transfers of Precise Location Data to Third Parties, or Third Parties' collection and use of Precise Location Data from or through a First Party's application with the First Party's affirmative authorization, for purposes other than those set forth in Section VI. Such notice should include clear descriptions of the following:

(a) The fact that Precise Location Data is transferred to or collected by any Third Party;

(b) Instructions for accessing and using a tool for providing or withdrawing Consent under Section IV.B with respect to the First Party's transfer of Precise Location Data to Third Parties and to the collection, use, and transfer of such data by any Third Party that the First Party affirmatively authorizes to collect Precise Location Data from or through the First Party's application; and

(c) The fact that the First Party adheres to these Principles.

First Parties should provide such notice on their own Web sites or accessible from the application from or through which the Precise Location Data is collected.

> *Commentary: Under Section IV.A.1, a First Party should provide notice of the fact that a Third Party collects data through the First Party's application where such data collection is affirmatively authorized by the First Party. First Parties are not required to provide further information about the Third Party's practices. Such further information should be provided in the Third Party's own notice as described in Section IV.A.2. For the purpose of this Principle, in instances where a Third Party may be collecting data from a First Party, where the First Party has not affirmatively authorized such collection, there is not an obligation on the First Party to provide notice of such collection.*

2. Third Party Notice

Third Parties should give clear, meaningful, and prominent notice of their Precise Location Data collection and use practices for purposes other than those set forth in Section VI. Such notice should include clear descriptions of the following:

(a) The fact that Precise Location Data is collected;
(b) The uses of such data, including whether it will be transferred to a non-Affiliate;

(c) Instructions for accessing and using the tool for providing or withdrawing Consent under Section IV.B with respect to the collection and use of such data or the transfer of such data to a non-Affiliate for purposes other than those set forth in Section VI; and

(d) The fact that the entity adheres to these Principles.

Third Parties should provide such notice on their own Web sites or accessible from any application from or through which they collect Precise Location Data.

3. First Party Enhanced Notice

In addition to providing notice as described in Section IV.A.1, First Parties should provide enhanced notice of Third Parties' collection and use of Precise Location Data from or through a First Party's application with the First Party's affirmative authorization, or a First Party's transfers of such data to Third Parties, for purposes other than those set forth in Section VI. Such enhanced notice should be provided as set forth below in (a) and (b) or through another method or combination of methods that provides equivalently clear, meaningful, and prominent enhanced notice:

(a) Notice of the Fact that Precise Location Data Is Collected: First Parties should provide clear, meaningful, and prominent notice of the

fact that the First Party transfers to any Third Party or authorizes any Third Party to collect Precise Location Data from or through the application:

(i) For a downloadable application, as part of the process of downloading an application to a device;

(ii) At the time that the application is opened for the first time; or

(iii) At the time such data is collected.

(b) Link to Disclosure: First Parties should provide notice through a clear, meaningful, and prominent link to the disclosure described in Section IV.A.1 that is presented:

(i) As part of the process of downloading an application to a device and before the application is installed, at the time that the application is opened for the first time, or at the time Precise Location Data is collected; and

(ii) In the application's settings or any privacy policy.

Commentary: A First Party can satisfy the requirement to provide download notice under Section IV.A.3.a by participating in a notice mechanism that satisfies this Principle and is offered by an application platform or an application market provider that makes the application available for download. For the purpose of this Principle, in instances where a

Third Party may be collecting data from a First Party, where the First Party has not affirmatively authorized such collection, there is not an obligation on the First Party to provide enhanced notice of such collection.

If a First Party elects to satisfy Section IV.A.3.a by providing a link within an application market that does not permit active links, the First Party satisfies this Principle if it provides an active link to a privacy policy that contains the disclosure described in Section IV.A.1 and directs consumers to the relevant section of the privacy policy where the disclosure is located.

B. CONSUMER CONTROL

1. First Party Consent

(a) Consent: First Parties should obtain Consent to transfer Precise Location Data to Third Parties for purposes other than those set forth in Section VI, or for affirmatively authorized Third Parties to collect and use Precise Location Data from or through the First Party's application or to transfer such data to non-Affiliates for such purposes. Such Consent tool should be easy to use and should apply to the application and device from which or for which the Consent is provided. The means for providing such

Consent should be described in the disclosure described in Section IV.A.1 above.

(b) Withdrawing Consent: First Parties should provide an easy-to-use tool to withdraw such Consent at any time, which should be described in the disclosure described in Section IV.A.1 above.

A First Party does not need to obtain such Consent in instances where the Third Party obtains Consent prior to collecting or using Precise Location Data for purposes other than those set forth in Section VI.

A First Party satisfies this Principle where it uses an easy-to-use process or setting offered by an application platform to provide notice, obtain Consent, and permit withdrawal of Consent with respect to the collection and use of Precise Location Data through the application for purposes other than those set forth in Section VI.

> *Commentary: Consent or a withdrawal of Consent under this Principle applies to future data collection, use, and transfer. A First Party is only subject to this Principle with respect to a Third Party's activities when it has affirmatively authorized the Third Party to collect the data. For the purpose of this Principle, in instances where a Third Party may be collecting data from a First Party, where the First Party has not affirmatively authorized such collection, there is not an obligation*

on the First Party to obtain Consent for such collection.

Multiple technologies can enable an entity to satisfy this Consumer Control Principle. For example, an entity can satisfy this Principle by allowing consumers to provide or withdraw Consent as a part of the process of downloading or installing an application, or through an application's settings. An entity may utilize permissions tools provided by an application platform or application market provider to satisfy this Principle. Specifically, for the purpose of this Principle, an entity can obtain Consent to the collection, use, and transfer of Precise Location Data through an individual's action in response to a clear, meaningful, and prominent notice provided under Section IV.A.3.a of the fact that Precise Location Data is collected from or through an application, assuming that the entity provides transparency as set forth in Section IV.A.

An entity that directs consumers to their device or platform settings, if such settings allow consumers to provide or withdraw Consent for the collection and use of Precise Location Data with respect to a specific application without changing their preferences for other applications, satisfies this Principle. An entity that offers an easy-to-use tool for consumers to remove that application from the

specific device from which such tool is accessed, and describes such tool in the disclosure described in Section IV.A.1, satisfies this Principle with regard to withdrawal of Consent under Section IV.B.1.b. Directing consumers to an application removal capability provided through a device's operating system is sufficient for this purpose if it allows consumers to remove or disable the application and to prevent any further collection of Precise Location Data from such device.

With respect to Consent for the collection and use of Precise Location Data by Third Parties, once a First Party has communicated the Consent or withdrawal of Consent to any Third Party that collects Precise Location Data through the application, the First Party has fully satisfied this Principle. The First Party obligation under this Principle results from the unique challenges of the mobile application context in those instances where it is not technically feasible for the Third Party to obtain such Consent.

Consent obtained by a First Party for the collection and use of Precise Location Data by a Third Party would constitute Consent to any subsequent use or sharing of such Data by the Third Party that is consistent with the notice provided, unless the First Party explicitly limits the terms of such Consent and provides for such limitations through a contractual arrangement with the Third Party.

2. Third Party Consent

Third Parties that collect and use Precise Location Data for purposes other than those set forth in Section VI, or transfer such data to non-Affiliates for such purposes, should obtain Consent or should obtain reasonable assurances that the First Party that provides the application obtains Consent to the Third Party's data collection, use, and transfer as set forth in Section IV.B.1 above.

> *Commentary: A Third Party obtains reasonable assurances as set forth in this Principle if the Third Party takes measures such as: (1) entering into a contract with the First Party under which the First Party agrees to obtain Consent to the Third Party's data collection and use; (2) obtaining other written assurances from the First Party to the same effect; (3) conducting periodic checks or audits of the First Party's Consent practices; (4) verifying that the First Party publicly represents that it obtains Consent to the transfer of Precise Location Data to a Third Party; (5) verifying that the First Party publicly represents that it adheres to these Self-Regulatory Principles; (6) verifying that the First Party obtains Consent to the collection of Precise Location Data and provides clear, meaningful, and prominent notice under Section IV.A.1 above that such data may be transferred to Third Parties; and/or (7) verifying that the First Party participates in a mechanism offered by a platform*

> *or operating system that provides the ability to obtain Consent that satisfies this Principle. A withdrawal of Consent applies to a Third Party if the Third Party has actual knowledge of the withdrawal.*

V. TRANSPARENCY AND CONTROL FOR PERSONAL DIRECTORY DATA

A Third Party should not intentionally access a device without authorization and obtain and use Personal Directory Data for purposes other than those set forth in Section VI.

A First Party should not affirmatively authorize any Third Party to intentionally access a device without authorization and obtain and use Personal Directory Data for purposes other than those set forth in Section VI.

VI. PURPOSE LIMITATIONS

Transparency and control should be provided for Cross-App Data, Precise Location Data, and Personal Directory Data as set forth in Sections III, IV, and V 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

(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 VI should not be used for a purpose other than those listed in Section VI without providing transparency and control as described above.*

VII. RESTRICTIONS ON USES FOR ELIGIBILITY PURPOSES

Notwithstanding any other provision, 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, promotion, 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.

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

VIII. SENSITIVE DATA

HEALTH AND FINANCIAL DATA

Except for operations or system management purposes, a Third Party should not collect and use Cross-App Data or Personal Directory Data containing financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records about a specific individual without Consent. Pharmaceutical prescriptions or

medical records that are de-identified as set forth in the HIPAA Privacy Rule, 45 C.F.R. § 164.514, are not limited by this subsection.

IX. DATA SECURITY

Entities should maintain appropriate physical, electronic, and administrative safeguards to protect Multi-Site Data, Cross-App Data, Precise Location Data, and Personal Directory Data.

X. ACCOUNTABILITY

The limitations and restrictions on the collection or use of Cross-App Data, Precise Location Data, and Personal Directory Data are within the scope of the Digital Advertising Alliance accountability programs.

* * *