DIGITAL ADVERTISING ALLIANCE RELEASES GUIDANCE ON THE APPLICATION OF ITS SELF-REGULATORY PRINCIPLES TO THE MOBILE ENVIRONMENT

Notice and Choice Required for Collection of Cross-Application, Precise Location, and Personal Directory Data

On July 24, 2013, the Digital Advertising Alliance (DAA), comprised of the largest media and marketing trade associations in the U.S., released new guidance regarding mobile and other devices (Mobile Guidance). The Mobile Guidance explains how the DAA’s existing Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles) and Self-Regulatory Principles for Multi-Site Data (MSD Principles) (together, the DAA Principles) apply to companies operating in the mobile ecosystem. It sets forth specific requirements for the collection and use of precise location information, as well as two new categories of data: “cross-app data” and “personal directory data.”

By articulating clear obligations for companies with respect to these types of data, the Mobile Guidance represents a milestone for the mobile advertising industry, which has been debating how to provide adequate notice and choice to consumers for quite some time. Noncompliance ultimately will be subject to the Online Interest-Based Advertising Accountability Program, operated by the Council of Better Business Bureaus. Participants in the mobile ecosystem—including app developers, analytics companies, ad networks, app platform providers, and providers of devices and related services—should evaluate their practices in light of the Mobile Guidance.

Background

In July 2009, the DAA published the OBA Principles, the online advertising industry’s effort to establish standard business practices concerning the collection of information about people’s online behavior across websites and its use in online behavioral advertising (OBA). They consist of seven principles, most notably requirements of clear notice to consumers about the collection and use of data for OBA purposes, and consumer choice regarding whether such data can be used for OBA. In 2011, the DAA expanded its self-regulatory program to cover “multi-site data,” which is all data collected from particular computers or devices regarding web viewing over time and across unaffiliated websites, and not just that collected for OBA purposes.

Mobile Guidance

The Mobile Guidance provides direction regarding how the DAA Principles apply within the mobile website and app environments. In particular, the Mobile Guidance:

• makes clear that the DAA Principles apply in the mobile context and elaborates on how they apply;
Digital Advertising Alliance Releases Guidance . . .
Continued from page 1...

- explains how the DAA Principles apply to data collected on a particular device regarding app use over time and across non-affiliate applications ("cross-app data");
- explains how the DAA Principles apply to data about the physical location of a device that is sufficiently precise to locate a specific individual or device ("precise location data"); and
- explains how the DAA Principles apply to the collection, use, and disclosure of calendar, address book, phone/text log, or photo/video data created by a consumer that is stored on or accessed through a device ("personal directory data").

The Mobile Guidance sets out responsibilities for “first parties” and “third parties.” A “first party” is an entity that owns or has control over an app with which a consumer interacts, as well as the entity’s affiliates. 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.¹

Application of Self-Regulatory Principles Across Channels

The Mobile Guidance first emphasizes that the DAA Principles apply consistently across all channels, regardless of the type of computer or device involved.² In commentary, however, the DAA acknowledges the technical limitations of different types of devices and systems. As a result, compliance with the DAA Principles in the mobile context may take a form different from compliance in the desktop computer environment, and implementation may vary based on the technological demands of other channels as well. The DAA anticipates providing further guidance on implementation practices.

Cross-App Data

Transparency

Under the Mobile Guidance, third parties should provide clear, meaningful, and prominent notice of their cross-app data collection and use practices. Such notice should be provided on the third parties’ own websites or accessible from any app from or through which they collect cross-app data.

Additionally, third parties should provide enhanced notice of their cross-app data collection and use practices by either using a notice in or around ads delivered using cross-app data (which can be satisfied through the use of the AdChoices icon) or in a number of ways that require the cooperation of the first party. If they do not provide enhanced notice in these ways, third parties should be listed individually on a mechanism or setting that meets DAA specifications and is linked from the first party’s disclosure. Third parties that obtain consent³ to their use and disclosure of cross-app data are not required to provide this enhanced notice.

Unless all third parties operating on the first party’s app have provided enhanced notice or have obtained consent to their cross-app data collection and use practices, any first party that affirmatively authorizes a third party to collect and use cross-app data also should provide notice in a specified time and manner.

Consumer Control

Third parties should provide consumers with choice regarding their collection and use of cross-app data and should describe those choice mechanisms in the relevant notices described above. Additionally, first parties that affirmatively authorize third parties to collect and use cross-app data should link to an appropriate choice mechanism.

The Mobile Guidance also provides that entities should not collect and use cross-app data through their provision of a service or technology that collects cross-app data from all or substantially all apps on a device without obtaining consent and providing an ongoing, easy-to-use means for users to withdraw such consent.

Precise Location Data

Transparency

For precise location data, the Mobile Guidance imposes requirements similar to those in the DAA Principles, but allocates responsibility differently to account for first parties’ greater ability to provide notice to consumers and obtain their consent in the mobile space.

First parties should provide notice of transfers of precise location data to third parties, as well as third parties’ collection and use of such data from or through the first party’s app and with the first party’s affirmative authorization. This notice should be on the first party’s website or accessible from or through the app from which precise location data is collected.

First parties should also provide enhanced notice regarding the collection and use of precise location data. The Mobile Guidance specifies permissible manners to provide such enhanced notice and notes that any method,

¹ Cross-app data also 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. It does not include (i) precise location data, (ii) personal directory data, (iii) data that has been de-identified in accordance with the Mobile Guidance, or (iv) data that is collected across unaffiliated apps but is not associated or combined across such apps.
² In situations where it is clear that the consumer is interacting with a portion of an app that is not an ad and is being operated by a different entity than the app owner, the different entity would not be a third party due to the consumer’s reasonable understanding of the nature of the direct interaction with that entity.
³ As a result of the consistent application of the DAA Principles across channels, the principles should be considered in connection with the collection of data from computers and devices, such as navigation devices and connected television devices in addition to mobile devices.
⁴ The Mobile Guidance, consistent with the DAA Principles, defines “consent” as “an individual’s action in response to a clear, meaningful, and prominent notice regarding the collection and use of data for a specific purpose.”

Continued on page 3...
or combination of methods, that provides equivalently clear, meaningful, and prominent enhanced notice is permissible.

Third parties should provide basic notice of their collection and use practices regarding precise location data on their own websites or accessible from any app from or through which they collect precise location data.

**Consumer Control**

First parties should obtain consent (i) for their transfer of precise location data to third parties, (ii) for affirmatively authorized third parties to collect and use precise location data from or through the first party’s app, and (iii) for their transfer of precise location data to non-affiliates. The first party should also provide an easy-to-use tool for users to withdraw such consent.

In addition, third parties should ensure that consent has been provided for their own precise location data practices, either directly or by obtaining reasonable assurances from the first party that it has obtained consent.11

Finally, the DAA notes in the Mobile Guidance that due to technical limitations of different devices and systems, it may not be feasible to comply with its guidance regarding precise location data on all devices in the same manner. The DAA may provide further guidance on implementation practices.

**Personal Directory Data**

The Mobile Guidance creates a new category of data, “personal directory data,” which 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.”12

The Mobile Guidance provides that third parties should not, without user authorization, intentionally access, obtain, and use personal directory data. Additionally, first parties should not affirmatively authorize any third party to do so.

**Exceptions and Specific Restriction on Uses for Eligibility Purposes**

The Mobile Guidance generally exempts first parties and third parties from their notice and choice obligations under the Mobile Guidance with respect to cross-app data, precise location data, and personal directory data that (i) is collected and used for specified purposes such as market research, product development, or operations and systems management, or (ii) has gone through, or within a reasonable period of time from collection goes through, an appropriate de-identification process. These exceptions are very similar to those contained in the MSD Principles. Also consistent with the MSD Principles, the Mobile Guidance specifies that, notwithstanding any of its other provisions, cross-app data, precise location data, and personal directory data should not be collected, used, or transferred for purposes of employment eligibility; credit eligibility; healthcare treatment eligibility; or insurance eligibility, underwriting, or pricing.

**Implications**

The Mobile Guidance likely will have significant ramifications for many participants in the mobile ecosystem. The FTC repeatedly has stated that the collection and use of information from mobile devices is one of its top agenda items because it believes consumers do not understand what collection is occurring and how they can control it. The Mobile Guidance provides companies in the mobile space with much greater clarity regarding how to provide the transparency and consumer choice demanded by the FTC and privacy advocates in the mobile context. Members of the organizations that comprise the DAA, as well as other companies within the mobile industry, are encouraged to examine the Mobile Guidance in connection with a review of their own practices concerning the collection, use, and disclosure of cross-app data, precise location data, and personal directory data.

Wilson Sonsini Goodrich & Rosati’s attorneys routinely counsel clients throughout the advertising ecosystem on self-regulatory requirements and other legal obligations relating to online behavioral advertising, and help clients manage risks relating to the collection, use, and disclosure of consumer data by mobile applications. For more information, please contact: Lydia Parnes at lparnes@wsgr.com or (202) 973-8801; Tonia Klausner at tklausner@wsgr.com or (212) 497-7706; Matthew Staples at mstaples@wsgr.com or (206) 883-2583; or any member of the firm’s privacy and data security practice.

---

11The Mobile Guidance lays out several illustrative actions that a third party may take to obtain reasonable assurances that a first party has obtained consent to its collection and use of precise location data. For example, a third party may obligate the first party contractually to obtain consent to the third party’s data collection or use, or may verify that the first party publicly represents that it obtains consent to the transfer of precise location data to a third party.

12Personal directory data also includes unique values assigned or attributed to a device or a unique combination of characteristics associated with a device, where combined with data, meeting the definition of 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.