Cooley

September 14, 2015

On September 1, 2015, the Digital Advertising Alliance ("**DAA**") began enforcing the application of its Self-Regulatory Principles for Online Behavioral Advertising and Multi-Site Data (the "**OBA Principles**", the "**MSD Principles**" and collectively, the"**Principles**")[1] to the mobile environment in accordance with the guidance it released in July 2013 ("**Guidance**").[2] As a reminder, the OBA Principles apply to the use of information collected from a particular device over time and across non-affiliate websites for the purpose of delivering online behavioral advertising and the MSD Principles apply to the use of the same data for other purposes such as adverse determinations concerning employment, credit, health treatment or insurance eligibility. As noted in this alert, the Guidance does not change the Principles but simply provides guidance on how the Principles are to be implemented given the technical demands of the mobile environment.

Companies that collect and use data across mobile sites or apps for interest-based advertising should review and consider complying with the Principles and the Guidance. The Council of Better Business Bureaus ("**CBBB**") and Direct Marketing Association ("**DMA**") will lead oversight of the independent accountability program. Complaints regarding companies that do not comply with the Principles can be reported to the CBBB's Online Interest-Based Advertising Accountability Program or the DMA's Ethics Operating Committee. Companies violating the Principles, even those that are not participants in the DAA's self-regulatory program, risk public announcement of any violations and being referred to the Federal Trade Commission or other regulatory authority for further action.

Overview of the Guidance and the Principles

Covered entities

The Guidance describes responsibilities of First Parties and Third Parties in collecting, using, and sharing data in the mobile environment. "**First Parties**" are entities and their affiliates that own or have control over consumer-facing applications. "**Third Parties**" are entities that collect data regarding application use over time and across non-affiliate applications ("**Cross-App Data**") or data obtained from a device about the physical location of the device that is sufficiently precise to locate a specific individual or device ("**Precise Location Data**") from or through a non-affiliate's application. Third Parties also include entities that collect from a device data that was created by a consumer and is stored on or accessed through the device such as calendars, address books, phone/text log, and photo/video data ("**Personal Directory Data**").

Multi-site data

The Guidance starts by noting that the collection and use of data collected from a device regarding web viewing over time and across non-affiliate websites ("**Multi-Site Data**") is subject to the MSD Principles[3], but the DAA recognizes that there are technical limitations to compliance on mobile platforms. For instance, on devices with small screens, it may not be feasible to provide notice of Multi-Site Data collection on the specific webpage 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 the notice to be provided where such notice is clear, meaningful, and prominent.

Transparency and control

The Guidance then delves into the specific responsibilities relating to transparency and control for Cross-App Data, Precise Location Data, and Personal Directory Data as set forth below. Transparency and control do not need to be provided for Cross-App Data, Precise Location Data, and Personal Directory Data if such data is used

solely for operations and system management purposes, market research and product development purposes, or where data has or will within a reasonable period of time from collection go through a de-identification process.

Cross-App Data

Third Parties should provide clear, meaningful, and prominent notice of their Cross-App Data collection and use practices ("**Cross-App Data Notice**"). Such notice should be on the Third Parties' own websites or accessible from any application from or through which they collect Cross-App Data.

The Cross-App Data Notice should include:

1. The types of data collected, including any personally identifiable information;
2. The uses of such data, including whether it will be transferred to a non-affiliate;
3. 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; and
4. The fact that the Third Party adheres to the Principles.

In addition, Third Parties who do not obtain consent prior to collecting or using Cross-App Data should provide enhanced notice. Enhanced notice is a clear, meaningful, and prominent link to the Cross-App Data Notice in or around ads delivered using Cross-App Data (which can be satisfied using the AdChoices icon). Alternatively, if the Third Party has an arrangement with the First Party, the Cross-App Data Notice should be provided in (i) the application's settings or in a privacy policy and (ii) 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. A Third Party that does not provide enhanced notice should be individually listed either on a mechanism or setting that meets DAA specifications that is linked to in a First Party notice or listed by the First Party in a list of Cross-App Data collectors.

When First Parties affirmatively authorize Third Parties to collect and use the Cross-App Data, the First Party should provide a clear, meaningful, and prominent link to a disclosure that either (i) points to a choice mechanism or setting that meets DAA specifications or (ii) individually lists such authorized Third Parties and provides consumers with the ability to exercise choice regarding their collection and use of Cross-App Data or the transfer of such data to non-affiliates. The link should be provided via (a) the application's settings or in a privacy policy and (b) 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. Where a Third Party is collecting data from a First Party, but the First Party has not affirmatively authorized such data collection, there is no obligation on the First Party to provide notice of such collection.

When providing a service or technology that collects Cross-App Data from all or substantially all applications on a device, companies should obtain consent from the user before collecting and using Cross-App Data. The consent should apply only to the device from which or for which the consent was provided. There should also be an easy-to-use means of withdrawing such consent.

Precise Location Data

First Parties should give clear, meaningful, and prominent notice of (i) transfers of Precise Location Data to Third Parties and (ii) Third Parties' collection and use of Precise Location Data from or through a First Party's application that received the First Party's affirmative authorization ("**First-Party Precise Location Data Notice**"). Such notice should be provided on the First Parties' own websites or accessible from any application from or through which they collect Precise Location Data.

In addition, First Parties should obtain consent to (i) transfer Precise Location Data to Third Parties, (ii) affirmatively authorize Third Parties to collect and use Precise Location Data from or through the First Party's application, or (iii) to transfer such data to non-affiliates. First Parties should also provide an easy-to-use tool to provide and withdraw consent. A First Party does not need to obtain consent when the Third Party has already obtained consent prior to collecting or using Precise Location Data. This consent requirement can be satisfied when a First Party uses a process or setting offered by an application platform to provide notice, obtain consent, and permit consent withdrawal.

The First-Party Precise Location Data Notice should include:

1. The fact that Precise Location Data is transferred to or collected by a Third Party;
2. Instructions for accessing and using a tool for providing or withdrawing consent 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
3. The fact that the First Party adheres to the Principles.

First Parties should also provide enhanced notice of such collection, uses, and transfers of Precise Location Data. Enhanced notice can be provided by a 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 as part of the process of downloading an application to a device, at the time the application is opened for the first time, or at the time such Precise Location Data is collected. This requirement can be satisfied by a notice mechanism offered by the application platform or application market provider that makes the application available for download. In addition, the First Party should provide a link to the First-Party Precise Location Data Notice (a) as part of the process of downloading an application and before the application is installed, at the time the application is first opened, or at the time Precise Location Data is collected and (b) in the application's settings or in a privacy policy. Enhanced notice can also be provided via another method or combination of methods that provides equivalently clear, meaningful, and prominent enhanced notice. Where a Third Party is collecting data from a First Party, but the First Party has not affirmatively authorized such data collection, there is no obligation on the First Party to provide notice of such collection.

Third Parties should also give clear, meaningful, and prominent notice of their Precise Location Data collection and use practices ("**Third-Party Precise Location Data Notice**"). Such notice should be on the Third Parties' own websites or accessible from any application from or through which they collect Precise Location Data.

Third Parties that collect and use Precise Location Data or transfer such data to non-affiliates should obtain consent or obtain reasonable assurances that the First Party that provides the application obtains consent to the Third Party's data collection, use, and transfer.

The Third-Party Precise Location Data Notice should include clear descriptions of:

1. The fact that Precise Location Data is collected;
2. The uses of such data, including whether it will be transferred to a non-affiliate;
3. Instructions for accessing and using the tool for providing or withdrawing consent with respect to the collection and use of such data or the transfer of such data to a non-affiliate; and
4. The fact that the Third Party adheres to the Principles.

Personal Directory Data

Third Parties should not intentionally access, obtain, or use Personal Directory Data without user authorization. First Parties should not affirmatively authorize the foregoing.

Data restrictions

Cross-App Data, Precise Location Data, and Personal Directory Data should not be collected, used, or transferred for determining employment, credit, health care treatment, or insurance eligibility or insurance underwriting and pricing. 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 prescription, 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 restriction.

In addition, while the Guidance does not specifically address the collection and use of personal information from children under the age of 13, the MSD Principles state that such information should only be collected and used in compliance with the Children's Online Privacy Protection Act.

Data security

Companies should maintain appropriate physical, electronic, and administrative safeguards to protect Multi-Site

Data, Cross-App Data, Precise Location Data, and Personal Directory Data.

Compliance tools

The DAA has released two tools—AppChoices and the Consumer Choice Page—to help companies comply with the Principles. AppChoices is an app, supported on iOS and Android, that permits consumers to opt out from the collection of Cross-App Data on a particular device for interest-based advertising and other applicable uses, by some or all of the companies listed in AppChoices. The Consumer Choice Page is a webpage that permits consumers to opt out from the collection of web viewing data for interest-based advertising and other applicable uses, by some or all of the companies listed on the page. If your company would like to participate in the AppChoices tool, you can request information from the DAA here. If your company would like to participate in the Consumer Choice Page, you can request information from the DAA here.

Notes

1. Digital Advertising Alliance, "Self-Regulatory Principles for Online Behavioral Advertising," 2009, and "Self-Regulatory Principles for Multi-Site Data," 2011.
2. Digital Advertising Alliance, "Application of Self-Regulatory Principles to the Mobile Environment," 2013.
3. The MSD Principles state that third parties and service providers that collect Multi-Site Data, or transfer such data to non-affiliates, for purposes other than online behavioral advertising should provide consumers with transparency and consumer control except for operations and system management purposes, market research or product development, or where the data will within a reasonable period of time from collection go through a de-identification process. The MSD Principles also set forth certain data use restrictions for employment, healthcare, credit, and insurance purposes and restrictions on child, health, and financial data.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Scott Dailard San Diego	sdailard@cooley.com +1 858 550 6062
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090

you should seek professional counsel.