COMPLIANCE WARNING REGARDING OBTAINING CONSENT FOR THE COLLECTION AND USE OF DATA FOR INTEREST-BASED ADVERTISING

CW-07-2022 – June 21, 2022

SUMMARY

The Digital Advertising Accountability Program (“Accountability Program”) issues this Compliance Warning regarding the practice of inferring Consent from a consumer’s passive use of a product or service before engaging in interest-based advertising (IBA). Specifically, the Accountability Program does not regard a consumer’s mere continued use of a product or service to satisfy the “action” component of “Consent” as defined by the Digital Advertising Alliance’s Self-Regulatory Principles for Online Interest-Based Advertising (DAA Principles). The DAA Principles require both a clear, meaningful, and prominent notice from the company and an action in response to that notice on the part of the consumer to obtain Consent under the Principles.

This warning will take effect on January 1, 2023.

The DAA Principles Describe Both Opting Out From and Consenting To IBA

The DAA Principles rest on the bedrock notion of providing consumers with transparency about and control over interest-based advertising. In many cases, this manifests in companies providing just-in-time notice on their websites, in their apps, or in or around their advertisements. That notice should lead to an explanation of the IBA activity at issue, and it should provide consumers with information about opting out of IBA. In such scenarios, data collection and use may proceed without need of any action by the consumer.

In some cases, however, the Principles require companies to obtain “Consent” prior to engaging in IBA. Consent is defined 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.”¹ In such situations, applicable data collection and use may only proceed after a consumer acts to allow it in response to the notice provided.

¹ Mobile Guidance § I.B; accord OBA Principles Definition D at 10.
Under the *OBA Principles*, “Action” is Required to Provide Consent, Not Inaction

The fact that the DAA Principles spell out different levels of consumer control in different situations indicates that they expect the practical results of those distinctions to be reflected in reality. In short, where Consent is required for certain data collection and use, companies may not proceed with such collection and use on what appears to be an opt-out basis.

To allow the word “action” to also encompass a lack of action would render “Consent,” as a specific requirement, superfluous. If “action” could be implicitly provided, such as by continuing to use a given app or website after being provided notice, there would be no difference between obtaining “Consent” and merely providing a notice that contains opt-out instructions. But the *OBA Principles* and *Mobile Guidance* define “Consent” specifically and require it, rather than a notice with opt-out instructions, under different circumstances.²

Depending on the circumstances, the Consent requirement can be satisfied in a number of ways. “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.”³ Additional provisions allow for Consent to be provided through device settings in some circumstances.⁴

Where “Consent” is Needed, it is an Independent Requirement from “Notice” and “Enhanced Notice”

While “Consent” is related to the concepts of “Notice” and “Enhanced Notice” found within the *Principles*, it is distinct from them. Consent is not merely a point on a continuum with Notice and Enhanced Notice; rather, each represents a discrete requirement that may be concurrently or independently invoked. As explained below, Notice and Enhanced Notice may point to a mechanism for providing Consent, but they cannot take the place of Consent.

² Specifically, Consent is required under the *Mobile Guidance* for Third Party “Cross-App Data Collection from All or Substantially All Applications,” § III.B.2, First Party transfer of “Precise Location Data to Third Parties” or for authorized Third Party collection and use of Precise Location Data, § IV.B.1, Third Party “collect[jion] and use [of] Precise Location Data,” § IV.B.2, or Third Party collection and use of Cross-App Data or Personal Directory Data, § VIII. By contrast, Notice is required for Third Party Cross-App Data collection and use, § III.A.1, in addition to Consent for First Party transfer of “Precise Location Data to Third Parties” or for authorized Third Party collection and use of Precise Location Data, § IV.A.1.

³ *OBA Principles*, Definition B at 4.

⁴ See, e.g., Mobile Guidance, Commentary, at 20 (“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.”); id., Commentary, at 27 (“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.”).
Let us begin with definitions. “Notice,” in the OBA Principles and Mobile Guidance, is a means of notifying users about the collection and use of data for IBA as well as explaining how to opt out of such collection and use. It is a core requirement under the OBA Principles and Mobile Guidance, fundamentally linked to the Principles’ other provisions. A typical example of a notice requirement from the Principles is as follows.

Third Parties and Service Providers should give clear, meaningful, and prominent notice on their own Web sites that describes their Online Behavioral Advertising data collection and use practices. Such notice should include clear descriptions of the following: (a) The types of data collected online, including any PII for Online Behavioral Advertising purposes; (b) The uses of such data, including whether the data will be transferred to a non-Affiliate for Online Behavioral Advertising purposes; (c) An easy to use mechanism for exercising choice with respect to the collection and use of the data for Online Behavioral Advertising purposes or to the transfer of such data to a non-Affiliate for such purpose; and (d) The fact that the entity adheres to these Principles.5

Next, “Enhanced Notice” is “a clear, meaningful, and prominent link” to a Notice.6 It is required in a number of circumstances and is most commonly seen in third-party advertisements, where it must be provided “[i]n or around the advertisement delivered on the Web page where data is collected; or [o]n the Web page where the data is collected if there is an arrangement with the First Party for the provision of such notice.”7

Consent, consisting of “an individual’s action in response to a clear, meaningful, and prominent notice regarding the collection and use of data for a specific purpose,” is specifically and exclusively invoked in situations requiring a heightened degree of consumer choice, such as: the collection of precise location data, particularly sensitive data, a material change in the use of prior-collected data, or the collection and use of data by a Service Provider for IBA.8

By the plain meaning and explicit construction of the Principles, then, Consent, Notice, and Enhanced Notice are independent requirements, and a company’s compliance with one requirement may be insufficient to show compliance with another. While we have not opined directly about these obvious distinctions in the context of collecting all or substantially all Multi-Site or Cross-App Data, we

5 OBA Principles § II.A.1.
6 See, e.g., OBA Principles § II.A.2(a).
7 Id.
8 See, e.g., Mobile Guidance § III.B.2 (regarding “Consent for Cross-App Data Collection from All or Substantially All Applications”); § IV.B.1 (regarding the First Party requirement for Consent “to transfer Precise Location Data to Third Parties”); § IV.B.2 (regarding the Third Party requirement for Consent to “collect and use Precise Location Data”); § VII (regarding the Third Party requirement for Consent to collect and use health and financial data); OBA Principles § III.B (regarding “Service Provider Consent for Behavioral Advertising”); § V (regarding the requirement for Consent prior to “Material Changes to Existing Online Behavioral Advertising Policies and Practices”); § VI.B (regarding the requirement for Consent prior to collecting health and financial data).
have clearly spelled out how these distinctions affect compliance in other Consent-requiring contexts. For instance, when “a mobile app publisher allows third parties to collect precise location data for IBA, it must provide users with the opportunity to give Consent to this collection, in addition to standard notice and enhanced notice of this fact.”\(^9\) Likewise, when data collection for IBA is occurring in the background of a mobile app, it is vital that first parties serve users with enhanced notice. This is especially true when sensitive data like precise location information is being collected, as consumers need to provide express Consent before this kind of data is collected by third parties for IBA.\(^10\)

Mobile app publishers that authorize the collection of precise location data for IBA must also provide notice, enhanced notice, and a Consent mechanism to their consumers. Publishers that collect personal directory data or personal information (PI) in the form of social security numbers or medical records information must obtain Consent from their users before using this information for IBA.\(^11\)

\[^9\] In re BPMobile LLC, No. 120-2020, at 1 (2020) (emphasis added).
\[^11\] In re iTriage, No. 64-2016, at 2 (2016).

Thus, no matter how repeated or prominent a company’s Notice or Enhanced notice may be, such Notice and Enhanced Notice cannot by themselves satisfy a requirement for Consent. A consumer must act in response to a clear, meaningful, and prominent notice, not merely receive one, for Consent to be real.

**Companies Mistake Inaction for Action, Fail to Get Consent**

The Accountability Program has noticed companies mistaking their provision of a notice combined with their customers’ subsequent continued use of their products or services as being tantamount to Consent. However, such reliance on the passive, continued use of a product or service just because it occurs subsequent in time to the delivery of clear, meaningful, and prominent notice is not sufficient to obtain Consent under the DAA Principles. Consumers must Consent through an action in response to these communications or some other compliant clear, meaningful, and prominent notice from the company. Without such action on the part of consumers, companies lack the needed Consent and
may not proceed with data collection and use for IBA in circumstances where the DAA Principles require it.

**The Accountability Program Will Strictly Require Consent for Certain Collection Activities**

The Accountability Program will strictly enforce the provisions of the DAA Principles requiring Consent. Where Consent is required, companies may not proceed with the covered activity on the subject device and/or application without obtaining that Consent. In seeking Consent, companies may not substitute a consumer’s inaction for action.

This Compliance Warning puts industry on notice of this enforcement activity. As of January 1, 2023, any entity found to be violating such provisions of the DAA Principles, and under the Accountability Program’s jurisdiction, is subject to enforcement action.