COMPLIANCE WARNING REGARDING FINGERPRINTING OF USERS OR DEVICES

CW-06-2022 – February 08, 2022

SUMMARY
The Digital Advertising Accountability Program (“Accountability Program”) issues this Compliance Warning regarding the practice of “fingerprinting” users or devices in connection with the collection or use of Cross-App Data. In enforcing the Digital Advertising Alliance’s Self-Regulatory Principles for Online Interest-Based Advertising (the “Principles”),1 the Accountability Program will treat any combined information used to uniquely identify a device or user for the purpose of interest-based advertising as equivalent to an Advertising ID in evaluating whether an entity is collecting or using Cross-App Data. This warning is effective immediately.

DISCUSSION
Under the Principles, “Cross-App Data is data collected from a particular device regarding application use over time and across non-Affiliate applications.”2 An entity collecting Cross-App Data and using it for Interest-Based Advertising (“IBA”)—or allowing another entity to do so—may need to provide Notice, Enhanced Notice, or Consent to the user, depending on the entity’s relationship to the user and the details of collection.3

Cross-App Data often includes the Android Advertising ID (AAID or IFA) or iOS’s Identifier for Advertising (IDFA) (collectively, “Advertising ID”), as a means of associating the use of a particular app with a particular device or user at a particular time. In its previous cases, the Accountability Program has treated an Advertising ID, in the context of a specific app and transmitted at a measurable time, as Cross-App Data.4 But Cross-App Data can include information suitable for identification other than the Advertising ID. When measurable characteristics gathered by an app, such as the volume, battery level, and IP address are combined, that data can be collected and used to tailor ads for that user/device. The use of device or user characteristics for such

---


2 Mobile Guidance § I.D.

3 Id. § III.

purposes is known as “fingerprinting.” While fingerprinting techniques have been used for years as a means of identifying web or mobile devices or users, they are increasingly relevant as access to other identifiers is restricted or narrowed.

The Accountability Program previously issued a Compliance Warning regarding such techniques in the context of website-based IBA. As that warning noted, the Principles are “applicable and will continue to be enforced irrespective of the technology employed to collect and use consumer web surfing activity to serve interest-based ads.” The Accountability Program reiterates that message and hereby restates it in the context of mobile devices.

Any unique combination of characteristics, when combined with Cross-App Data (which may consist simply of an app identifier transmitted at a particular time) is itself Cross-App Data. Accordingly, for enforcement purposes, the Accountability Program will treat any combined information used to uniquely identify a device or user for IBA as equivalent to an Advertising ID in evaluating whether an entity is collecting or using Cross-App Data. Such information may include, but is not limited to, the device IP address, platform, brand, model, carrier, OS version, screen resolution, processor, or language settings, whether collected at once or over multiple sessions.

CONCLUSION
Entities engaged in IBA must adhere to the Principles’ self-regulatory requirements regardless of the technologies they employ. Moreover, entities that use fingerprinting techniques to identify users or devices for IBA are required to provide the same level of transparency and choice to consumers as they would if using an Advertising ID for the same purpose. The Accountability Program seeks to remind industry of its obligations and to demonstrate that in this era of rapid change, self-regulation can and will respond promptly to new technologies and trends.

---


7 Id. at 1.

8 Mobile Guidance § I.D., Commentary, at 5.