Today’s Speaking Faculty

Jon Brescia, Director, Adjudications and Technology, Advertising Self-Regulatory Council (ASRC) and Council of Better Business Bureaus (CBBB) | @bbb_us

Michael A. Signorelli, Partner, Venable LLP, and Counsel, Digital Advertising Alliance (DAA) | @VenableLLP

Chris Yamaoka, General Counsel & Chief Privacy Officer, GroundTruth | @GroundTruthCo

Moderator and Introductions: Lou Mastria, CIPP, CISSP, Executive Director, Digital Advertising Alliance (DAA) | @DAAUSA @lmastria
Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it’s anonymous, but the data shows how personal it is.

House Republicans Demand Answers On Location Privacy
Mobile Accountability

• Enforced since September 1, 2015
• DAA Enforcement Partners: Council of Better Business Bureaus and the Data Marketing and Analytics (DMA) Division of Association of National Advertisers
• Active monitoring of First Parties & Third Parties
• Supplemented by Complaint-based system
• Independent of DAA
• Take-aways for All Parties | Keeping Mobile Apps & Ads “Safe”
The DNA of DAA
DAA Principles Cover Interest-based Advertising and Multi-site Data Collection

https://www.digitaladvertisingalliance.org/principles

Enforcement provided by CBBB and DMA
Why DAA Principles & Program Matter

- The DAA Principles are a helpful cornerstone for a privacy program.
- Externally, they provide a common language for conversations with partners in the ecosystem.
- Internally, they provide a starting point for essential conversations with key stakeholders.
- The DAA Program helps us understand our role as a first party and a third party in the collection, use and application of user data for IBA purposes.
Reminder: What Does DAA Mobile Guidance Require of Us

Application of Self-Regulatory Principles to the Mobile Environment

• This guidance explains how the existing IBA Principles and MSD Principles (the DAA Principles) apply to certain types of data in the mobile Website and application environment.
Guidance for Four Specific Mobile Data Types

This guidance responds to the fact both First Parties and Third Parties operate across a variety of channels, including mobile. As advertisers and consumers go multi-screen, so does DAA.

Addresses First- and Third-Party obligations with respect to the following data practices:

1. Multi-Site Data
2. Cross-App Data
3. Precise Location Data
4. Personal Directory Data
Understanding Your Role in Mobile Data Types

**First Party:** An entity that is the owner of an application, or has control over the application, with which the consumer interacts, and its Affiliates.

**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.

Note whether a party is a first party or a third party depends on its function in particular circumstances.
Precise location: Things to consider at development

• Likely, you are thinking about a million things at development, including how to monetize the app

• If ads, will you be allowing Interest-Based Advertising (IBA)?

• If so, you have responsibilities under the DAA Principles

• Today, we will be focusing on your responsibilities with respect to Precise Location Data
What is precise location data (PLD)?

The Mobile Guidance defines precise location data, or PLD, as the following:

Precise Location Data is data obtained from a device about the physical location of a device that is sufficiently precise to locate a specific individual or device.
Step 1: Do I want to?

- The first step in using PLD in IBA is asking whether you **want to do so at all**
- Not all businesses are interested in doing so, so think about it first.
- Let’s assume you decide to go ahead
Step 2: Get compliant

- If you are authorizing the collection of PLD for IBA, there are two broad areas to consider:
  - Privacy disclosure changes
  - User experience changes (enhanced notice and consent tools)
- We’ll walk through all of these from start to finish to help you understand what goes where—and when!
Privacy policy: PLD notice

• First thing’s first: you’ve decided to allow collection of PLD for IBA, so you should update your privacy policy to meet the notice requirement.

This notice must be placed on the company’s website or be accessible through its app(s) and provide clear descriptions of: (1) the fact that precise location data is transferred to or collected by any third party, (2) instructions for accessing and using a tool for providing or withdrawing consent, (3) and the fact that the first party adheres to the DAA Principles.

• This policy is the bedrock of your compliance process, as your enhanced notice will need to point to it.
Enhanced notice for PLD

• Besides your PLD notice, you also need **enhanced notice**. Enhanced notice is notice at the **right place and the right time**

• For PLD enhanced notice, section IV.A.(3)(a) requires:

Enhanced notice is a clear, meaningful, and prominent notice of the fact that the first party authorizes third-party collection of precise location data (or transfers such data to third parties). The enhanced notice must be provided during the process of downloading the application, at the time the application is opened, or at the time such data is collected. Companies may use features built into an app store or app platform to provide this enhanced notice.
Enhanced notice for PLD

- And section IV.A.(3)(b) requires:
  
  First parties must link to their PLD notice during the process of downloading the application (pre-install), at the time the application is opened, or at the time such data is collected AND in the application’s settings or any privacy policy.

- Companies may also supply their own method of enhanced notice as long as it is equivalently clear, meaningful, and prominent
Enhanced notice for PLD

• Practically speaking, this suggests 3 obvious options for **enhanced notice**, all having to occur no later than the moment of first collection

  1. App store
  2. Custom dialogue on first run
  3. When PLD data is first collected

• You’ll also need to ensure folks can reach an enhanced notice link through your app settings or any privacy policy
1. App stores & enhanced notice

- You control what you put in the app store fields—descriptions, links, and other vital info.

- So, your app’s page in the store is a great place to give enhanced notice. There are multiple ways to do so, but let’s look at a common way...
From the **privacy policy link** on your app’s app store page... to the **top of the privacy policy** where a location-related jump link is placed... that takes people from the top of your policy **directly to** the relevant section.

---

**Section IV: Location**

We may use location. It may be precise. Third parties may get it for ads. They will find you. They know.

For information about our location data policies, **click here**.

Section I.

For information about interest-based advertising and your choices, **click here**.
2. Custom dialogue & enhanced notice

• Another option some developers use is a pop-up dialogue box on first run.

• This dialogue box can direct users to your PLD disclosure.

---

Public Transit!

Your Location

Welcome to our app! We need your location data for our app to work. We also let our advertising partners know where you are so that they can provide you with relevant ads. For information about our location policies, please tap here.

Section IV: Location

We may use location. It may be precise. Third parties may get it for ads. They will find you. They know.

You can turn off location permissions on an app-by-app basis. Learn how by clicking here for Android or here for iOS.
3. First collection & enhanced notice

- Another option is when PLD is collected for the first time
Enhanced notice: Additional points

• No matter which solution you choose, **you must also** place an enhanced notice link in your “application’s settings or any privacy policy”

• A best practice is to use the AdChoices Icon in your enhanced notice
Obtaining consent

• **Consent** is a critical part of compliance with the Mobile Guidance

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.
Obtaining consent

• **Do not** just use the default system prompt without additional language

• **Edit it to describe third party IBA!** Or alternatively, use a custom prompt
Obtaining consent: Modified permissions examples

- WeatherBug’s iOS consent flow starts with a custom dialogue box, which you can see in the background of these images.

- The app also provides two customized iOS permissions prompts that explain the reasons they are requesting location permissions.
Obtaining consent: Custom box and enhanced notice

- If you can’t modify the permissions tool, you can explain to consumers what they are consenting to using the same custom dialogue box that contains your PLD enhanced notice link.
- This explanation should come before the system permissions tool that actually allows users to consent.
- Then, consumers can consent to the collection of location using the standard permissions tool.
Consent withdrawal

- Consent can be revoked after it is given, and the Principles expect you to provide an easy-to-use tool to users in your PLD notice.
- If people want to revoke consent, they will often need to change the permissions settings in their apps.
- Show them how or point them to authoritative guides that do.
- Another way is having users uninstall the app.
- But you can’t just tell people to turn off GPS globally—must be on an app-by-app basis.
- By far, the common of these that we have seen app publishers employ is the OS instructions option.
By enabling Location Services for your devices, you agree and consent to the transmission, collection, maintenance, processing, and use of your location data and location search queries by Apple and its partners and licensees to provide and improve location-based and road traffic-based products and services.

The crowd-sourced location data gathered by Apple does not personally identify you.

You may choose to disable Location Services at any time. To do so, open Settings on your iPhone, tap Privacy, tap Location Services, and either turn off the global Location Services switch or turn off the individual location switch of each location-aware app or feature by setting it to “Never”. To disable Location Services for all websites, set the Location Services setting for Safari to “Never”. You may also disable location-based system services by tapping on System Services and turning off the switch for each location-based system service. You may choose to disable Location Services for your HomePod at any time in the HomePod settings in the Home App on your paired iOS device.

If you allow third-party apps or websites to use your current location, you are subject to their terms and privacy policy and practices. You should review the terms, privacy policies, and practices of such apps and websites to understand how they use your location and other information.

Information collected by Apple will be treated in accordance with Apple’s Privacy Policy, which can be found at www.apple.com/privacy
Consent withdrawal: Instructions

Android: For 6.0 and above: [https://support.google.com/googleplay/answer/6270602](https://support.google.com/googleplay/answer/6270602)
For earlier versions of Android: [https://support.google.com/googleplay/answer/6014972](https://support.google.com/googleplay/answer/6014972)
A note for our ad tech friends

• As a third party, you are not exempt from the PLD requirements
• You have different obligations
• This includes notice, consent revocation, and obtaining reasonable assurances from first parties
• Make sure you
  • Provide a PLD disclosure
  • Obtain consent or reasonable assurances from publisher partners that consent has been obtained **prior to collecting PLD**
  • Explain to consumers how they can withdraw consent
Other compliance tips

• PLD is big, but cross-app is bigger; it’s the backbone of IBA in mobile and comes with its own notice, enhanced notice, and opt-out requirements
• Make sure your terms are up front about what you do
• Check the contracts you’re signing—compliance can sometimes be a bonus in that it prevents you from breaching vendor agreements
• Websites still exist! The web—accessed from mobile or traditional desktop machines—is subject to the OBA Principles, which require transparency and consumer control for IBA, among other things. If you run a website that allows IBA, you can use footer notice to provide enhanced notice
• Third parties: you have websites, and in that context, you are also first parties!
Other compliance tips

• **Don’t forget cross-device!**
• We have had two cases on this point so far, LKQD and Kiip
• Both were complicated cases tackling multiple issues
• Enhanced notice, consent, etc. are obviously important, but the Cross-Device Guidance requires **specific disclosures** if you engage in cross-device IBA, and you’ll need the whole package to be fully compliant
Accountability Program ‘Season 8’ (2019) Underway

• A total of 97 formal actions to date
• New consumer complaint form launched
• Enforcement in Action 3.0: https://www.digitaladvertisingalliance.org/casebook
• Well over 17,000 consumer queries fielded
• VIRTUALLY 100% VOLUNTARY COMPLIANCE – SELF-REGULATION WORKS
DAA Resources | https://www.digitaladvertisingalliance.org/resources

FIRST-PARTY
Implementation Guidance

- Mobile App Guidance
- Websites & Mobile Web Guidance

THIRD-PARTY
Implementation Guidance

- Mobile App Guidance
- Websites & Mobile Web Guidance
Questions | Thank You! | See you at www.daasummit19.org

Jon Brescia, Director, Adjudications and Technology, Advertising Self-Regulatory Council (ASRC) and Council of Better Business Bureaus (CBBB) | @bbb_us

Michael A. Signorelli, Partner, Venable LLP, and Counsel, Digital Advertising Alliance (DAA) | @VenableLLP

Chris Yamaoka, General Counsel & Chief Privacy Officer, GroundTruth | @GroundTruthCo

Moderator and Introductions: Lou Mastria, CIPP, CISSP, Executive Director, Digital Advertising Alliance (DAA) | @DAAUSA @Imastria