Data Privacy Monitor
Commentary on Data Privacy & Information Security Subjects

BakerHostetler

Increased Scrutiny on Notice and Choice for Use of AD Profiling, Especially Using Mobile Location Data



By **Taylor A. Bloom**, **Alan L. Friel** and **Niloufar Massachi** on March 20, 2019
Posted in **Advertising, Big Data, Marketing, Mobile Privacy**

Are you an app publisher or do you advertise via mobile apps or obtain marketing data that originates from them? If so, you need to beware that regulators and consumer protection authorities are taking action against companies with regard to the notice and choice, or lack thereof, they are providing to consumers for the collection of their precise location data on mobile devices. The Digital Advertising Alliance (DAA) recently held a presentation (DAA Presentation) which highlighted what transparency and choice consumers should be provided in connection with the collection of such location data. Among the speakers was Jon Brescia, Director of Adjudications and Technology of the Advertising Self-Regulatory Council (ASRC) Online Interest-Based Advertising Accountability Program (OIBAAP), which enforces the DAA's self-regulatory principles. For one, the DAA requires that consumers be provided enhanced notice of location awareness for advertising purposes during the process of downloading the mobile 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. Based on conversations we have had with the OIBAAP, and suggestions made during the DAA Presentation, enhanced notice can be provided ether in the precise location data permission box of the mobile application or in a pop-up that

appears immediately before the permission box is displayed. This is consistent with the position taken by the Los Angeles city attorney in a lawsuit regarding a commercial mobile application discussed below. Companies should evaluate the adequacy of the notice and choice they are providing to consumers and supplement their practices where necessary to meet self-regulatory best practices and avoid becoming the subject of an enforcement action or a lawsuit.

Self-Regulatory Recommendations:

The DAA establishes and enforces privacy practices for digital advertising. **The ASRC,** administered by the Council of Better Business Bureaus, establishes the policies and procedures for advertising industry self-regulation, including the Online Interest-Based Advertising Accountability Program (OIBAAP), which bases its enforcement standards on the DAA's self-regulatory codes and principles (DAA Principles), which are enforceable against any publisher, advertiser or related intermediary. Further, the Network Advertising Initiative (NAI) sets forth self-regulatory codes that are enforceable against all NAI member companies (NAI Principles) (who must agree to uphold the NAI Principles in order to qualify for membership), which in turn require publishers and advertisers they work with to also comply with the NAI Principles.

The DAA Principles require notice be provided to consumers that their data regarding their usage activities may be collected by third parties over time and across services, and/or that their cross-device usage and/or precise location may be tracked, and that such data may be used for interest-based advertising (IBA), including for retargeting. Required notices include both notice in privacy policies and certain enhanced notice requirements. According to input we have received from the OIBAAP, privacy policies should have a jump link at the top directing consumers to where they can learn more about how they can exercise certain choices regarding IBA through the DAA/NAI opt-out programs, and include a statement that the company supports the self-regulatory principles. However, we recommend that privacy policies make clear that the company is not responsible for the effectiveness of, or compliance with, any third-parties' (e.g., DAA and NAI) opt-out programs or the accuracy of their statements regarding their programs. The DAA's self-regulatory program also requires companies to add an enhanced notice link in the footer or header of every website page with which IBA is associated that deep links to the section of the company's privacy policy where there is a description of and further link to an IBA opt-out opportunity. If a service tracks precise location for advertising, or otherwise shares precise location information with third parties, the OIBAAP expects that it include enhanced notice of that before asking for access to precise location. As explained above, this can be done by means of a pop-up before the location permission box of the two dominant mobile operating systems (OS) is presented on the mobile application or by customizing the permission box. The OIBAAP would prefer that the disclosure have a link to the more detailed disclosure and opt-out link in the privacy policy, although the DAA Principles do not expressly require this. Both of the dominant mobile OS provide instructions to users on how to use OS controls, which we suggest app publishers link to these in the location tracking section of their privacy notices. For mobile, the OIBAAP expects enhanced notice of IBA generally, of any cross-device tracking for IBA, and of any collection of precise location IBA or otherwise for third parties to be, at minimum, noted in the top half of the first page of the privacy policy, with a jump link to the fuller explanation and a link to the DAA opt-out page.

The DAA and OIBAAP expect that publishers and advertisers will only work with IBA vendors that accept and abide by the DAA's principles. In enforcing the DAA Principles, the OIBAAP independently seeks out noncompliance and brings enforcement actions against publishers, advertisers and their intermediaries. None of the DAA, ASRC or OIBAAP have the power to issue penalties, but the OIBAAP does publicly publish their findings and has in the past made referrals to the Federal Trade Commission (FTC) to investigate practices that might be deceptive or unfair under the FTC Act.

Self-Regulatory Authority Investigation:

On Jan. 28, 2019, the OIBAAP released a new decision resulting from consumer complaints filed with the Better Business Bureaus, which demonstrates the program's efforts to bring publishers into compliance with the DAA Principles, including by providing enhanced notices to consumers. The OIBAAP began investigating a publisher's privacy practices after receiving consumer complaints, and its inquiry determined that the publisher's "homepage allowed third-party advertising companies to collect data for targeted advertising but did not provide real-time, 'enhanced' notice to end users." Further the OIBAAP also found that "a third-party company was collecting precise location data through one of the publisher's mobile apps, raising a possible issue with the publisher's compliance with" the DAA's mobile guidelines. According to the OIBAAP, the publisher immediately committed to complying with the DAA Principles upon receiving the inquiry letter and worked to remedy the issues identified, by doing the following:

- "Updat[ing] its website footer to provide enhanced notice to its website visitors.
- Modif[ying] its privacy disclosures so users could receive enhanced notice when they visited its mobile apps' pages in the…app stores.
- Updat[ing] the relevant mobile app to disable collection of precise location data by third-party advertisers, as the company never intended for this to occur and was unaware that this collection had been occurring."

These remediation commitments should guide companies in their IBA notice and choice practices.

The Weather Channel Lawsuit

Los Angeles City Attorney, Michael Feuer, recently brought a lawsuit against The Weather Channel (TWC) on behalf of the people of the state of California for serving geolocation-specific advertisements through its mobile application (app) without allegedly sufficient notice and consent. *The People of the State of California v. TWC Product and Technology, LLC*, Los Angeles Superior Court Case No. _ (filed Jan. 3, 2019) (complaint). The suit is being brought under California's Unfair Competition Law (the UCL) as an unfair and deceptive practice. California Business and Professions Code Sections 17200 et seq. The suit asserts that TWC "deceptively collected, shared and profited from the location information of millions of American consumers," using their data for practices such as targeted marketing and hedge fund analysis.

The city attorney's claim of insufficiency of transparency and choice is brought notwithstanding that the app's privacy policy and settings disclose that geolocation may be shared with third parties for commercial

purposes and used for advertising. The complaint alleges that since the pop-up request for consent to track location (a requirement of the two dominant mobile OS) does not explain these uses, nor does the app's description in the app store, the privacy policy and settings disclosures are inadequate, because users would not have "any reason to believe that their location will be used for anything other than personalized local weather, data, alerts and forecasts. Users therefore have no reason to seek such information by combing through the app's lengthy 'Privacy Policy' and 'Privacy Settings' sections – buried in each of which are opaque discussions of TWC's potential transmission of geolocation data to third parties and use for additional commercial purposes. Indeed, on information and belief, the vast majority of users do not read those sections at all."

In other words, the theory of the case is that it is a deceptive and unfair practice under California law to rely on consent to enable location awareness generally and a disclosure of the advertising and other commercial uses of that data collection in the privacy policy, rather than to provide far more clear, conspicuous and proximate notice of the data practices. If successful, this case could move transparency and choice best practices to a legal baseline, and in doing so alter the way many website and mobile app publishers provide notice of things like interest-based and location-aware advertising. It could also open the litigation floodgates, since the UCL permits class actions by private plaintiffs.

The suit seeks civil penalties of up to $2,500 for each violation of the UCL. In these cases, a judge determines the number of violations and the amount of the penalties based on the AG's recommendations, but the number of incidents could be calculated broadly based on number of users and data uses, in which case the potential penalties could be enormous. This case reflects a growing trend of increased sensitivity by consumers, lawmakers, regulators and consumer protection authorities regarding the ways companies collect, use and share consumer data, and what transparency and choice they provide data subjects. It also demonstrates that even without specific privacy legislation such as that recently passed by California (see our prior posts here and here), state and local prosecutors, and in many states private plaintiffs, may be able to challenge commercially commonplace data practices under state unfair and deceptive practices acts and other consumer protection laws of general application.

Although we do not necessarily agree with the city attorney that a failure by TWC to provide more specific particularity around its geolocation practices constituted deceptive or unfair practices, considering the position the city attorney has taken, we recommend that companies consider adopting some kind of enhanced notice. For instance, as suggested by the Los Angeles city attorney, the description of the app in the app store could explain that the app is ad-supported and uses the user's location to send location-relevant ads. Consistent with the recent DAA/ASRC/OIBAAP recommendations, there should be enhanced in-app notice as part of the app download and onboarding process, such as use of a pop-up or push notification. Publishers may even be able to provide a customized location permission request alert. One of the dominant OS allows apps to provide a custom text known as a purpose string or usage description string for display in the system's permission request alert. While many apps in the United States lack custom language around location in the permission request, we have seen a higher level of particularity within these requests in the EU. For example, many EU app disclosures state that location will be used for

"geographically relevant ads." This is not surprising, since EU law, unlike U.S. law, specifically requires explicit consent to collection and particular uses of geolocation data. Here, TWC did use a custom permission request alert, which stated, "Allow 'The Weather' to access your location? You'll get personalized local weather data, alerts and forecasts." If that notice had included "and location-relevant ads," that might have been enough for the company to avoid the claims of inadequate notice and choice.

It is significant to note that this is not the first case of this kind. The FTC and other states have brought similar actions against companies for deceptive business practices around disclosures of location tracking practices. Prior cases, however, have involved publishers providing an opt-out from GPS location tracking while continuing to track location using other methods such as Wi-Fi tower proximity, and not explaining to users that the opt-out really did not stop location tracking, just merely one form of it. Those cases are markedly different from the Weather Channel case, which is really about enhanced notice. We will monitor this case and report on how it progresses.

State and Federal Guidance:

The California attorney general issued guidance in 2013 on recommendations for mobile app privacy notice and practices – "Privacy on the Go." The FTC published similar guidance also in 2013 – "Mobile Privacy Disclosures, Building Trust Through Transparency." The guidance provided by the California attorney general recommends providing a notice that location data will be collected, and an option to allow or prevent the practice. Similarly, the FTC recommends providing a "just-in-time disclosure to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation." While both are mere recommendations and not regulatory requirements, companies should review their website and mobile app privacy practices and notices and take these recommendations into consideration in deciding whether they need to provide more enhanced notice or greater data subject control.

While TWC appeared to be following the recommendations from the California attorney general and the FTC regarding mobile app privacy and providing notice of location tracking practices, the Los Angeles city attorney is seeking a level of transparency beyond even what the attorney general and FTC have suggested as best practices. Interestingly, in December, a major social media platform was fined under a similar action in Italy. The fine was not brought by the Italian Data Protection Authorities, but instead was issued by the Italian Competition Authority (ICA). The ICA found the social media platform to be in violation of Articles 21 and 22 of the Italian Consumer Code for misleading consumers about how their data will be used for commercial purposes. Accordingly, there appears to be a worldwide trend of applying consumer protection laws of general application to data practices. The standards for measuring deception and unfairness when it comes to transparency and choice may be evolving.

Takeaway

Enhanced transparency and choice are necessary to meet self-regulatory requirements and will help avoid potential unfair practice claims. Companies should evaluate the ways they give notice of data practices,

especially those that might arguably be unexpected by data subjects, and consider when and how to give enhanced notice and choice. For more information, contact the authors.