Bloomberg BNA

Electronic Commerce & Law Report™

ONLINE ADVERTISING

Two recent actions against mobile application developers, for allowing third parties to collect user data for advertising purposes, highlight a trend of increasing privacy enforcement within the industry. Attorneys from WilmerHale discuss the trend and suggest ways in which developers can ensure compliance with relevant guidance from the Digital Advertising Alliance and Federal Trade Commission.

Self-Regulatory Actions Signal Warning for Mobile Apps That Allow Third Parties to Collect Information for Interest-Based Advertising

BY D. REED FREEMAN AND PATRICK BERNHARDT

Recent actions against two prominent mobile app developers serve as a warning for companies that authorize third parties to collect and use information over time for advertising in mobile apps (known as interest-based advertising or IBA). On July 14, the Council of Better Business Bureaus' Online Interest-Based Advertising Accountability Program issued two formal decisions against SEGA and iTriage LLC, case numbers 64-2016 and 65-2016 respectively, for alleged violations of the Digital Advertising Alliance's (DAA) Self-Regulatory Principles in the mobile environment. *See* Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (July 2013) (''Mobile Guidance'').

D. Reed Freeman, Jr. is a partner at Wilmer Cutler Pickering Hale and Dorr LLP. He is a leading authority on privacy, cybersecurity, and online, mobile, and social media advertising and privacy law. Mr. Freeman serves as co-chair of the firm's Cybersecurity, Privacy and Communications Practice. He can be reached at reed.freeman@wilmerhale.com.

Patrick Bernhardt is an associate in the Cybersecurity, Privacy and Communications Practice at Wilmer Cutler Pickering Hale and Dorr LLP. He advises companies on a broad range of US and international privacy, consumer protection and data security laws. He can be reached at patrick.bernhardt@wilmerhale.com.

Along with other recent developments, these actions show that self-regulatory programs—and regulators such as the Federal Trade Commission (FTC)—now expect companies to provide adequate notice and choice for interest-based advertising in mobile apps. The Accountability Program will bring actions against any website or mobile app that is engaged in IBA, regardless of whether the company expressly adheres to the DAA's Principles. More broadly, these actions highlight a trend of increasing privacy enforcement in mobile apps and other emerging online advertising technologies.

Alleged Failures to Comply With DAA's Mobile Guidance

In its decisions, the Accountability Program alleged that SEGA's ''Sonic Runners'' mobile gaming app and a health app called ''iTriage,'' owned by a subsidiary of Aetna, allowed third parties to collect and use information (including iTriage users' in-app behavior such as the features and tools used) for IBA purposes, without providing adequate notice and choice under the DAA's Mobile Guidance. For example, the decisions alleged that the companies failed to adequately disclose third-party IBA practices in their privacy policies.

The companies also allegedly failed to provide so-called ''enhanced notice'' outside of the privacy policy to alert users that information collected through apps would be used for IBA purposes. Under the DAA's Mo-

 ISSN 1098-5190

bile Guidance, companies must provide such enhanced notice either prior to download (*e.g.*, in the app store on the application's page), during download, on first opening of the app, or at the time data is first collected *and* in the application's settings or privacy policy.

According to the decisions, the mobile apps also allowed third parties to collect precise location data (*e.g.*, latitude and longitude coordinates derived from GPS or Wi-Fi network signals on a user's mobile device) for IBA purposes without obtaining consumers' affirmative consent. In particular, the Accountability Program noted in its decision against iTriage that the app's settings may be used to obtain consent only ''if they satisfy the actual requirement, *e.g.*, provide notice of transfer of location data to a third party for IBA.'' *In re iTriage* at FN 35. In other words, if mobile apps rely on the platform-provided consent mechanisms in iOS or Android, the consent language must specifically disclose the fact that location data will be passed to third parties for IBA purposes.

Finally, the decisions made it clear that the Accountability Program's staff will review companies' practices with respect to *all* types of information collected or used for IBA purposes, including personal directory data (such as contacts, calendars, or photos on a user's device), health data, children's data, and other sensitive data. For example, in its decision against SEGA, the Accountability Program concluded that SEGA allowed third parties to collect information about children under the age of 13 without obtaining verifiable parental consent, in violation of the Children's Online Privacy Protection Act (COPPA).

Increasing Privacy Enforcement in Mobile Apps

The actions against SEGA and iTriage demonstrate the industry's willingness to ramp up self-regulatory enforcement in mobile apps to keep pace with the FTC's increasing interest in mobile privacy. These actions follow quickly after the Accountability Program's first-ever enforcement actions against mobile app developers in May 2016.

In addition, the Network Advertising Initiative (NAI), a membership organization for third-party advertising service providers, has started to examine during its annual compliance reviews whether members are complying with the NAI Mobile Code. *See* Network Advertising Initiative, *2015 Update to the NAI Mobile Application Code* (Aug. 2015). Accordingly, many companies have been updating their privacy policies and practices in mobile apps to comply with the DAA and NAI mobile guidance.

For its part, the FTC also has demonstrated its willingness to bring enforcement actions against companies that allow or engage in targeted advertising in mobile apps. For example, in June 2016, the FTC entered into a settlement with a mobile advertising network for allegedly collecting users' precise location in a manner that bypassed the location settings on users' mobile devices (*United States v. InMobi Pte Ltd.*, N.D. Cal., No. 3:16-cv-03474, *stipulated order filed* 6/22/16).

The FTC also fined the company $950,000 for collecting information from mobile apps directed to children without obtaining verifiable parental consent as required under COPPA. *Id.* This settlement is just the latest in a series of FTC privacy enforcement actions against mobile app developers and their third-party partners.

Key Takeaways

Mobile app developers should review their practices and ensure that they comply with relevant DAA and FTC guidance before they allow third parties to collect and use information through mobile apps for IBA purposes. In particular, companies can review the Accountability Program's compliance tips and take the following additional steps:

- confirm whether you authorize third parties to collect or use information on websites *or in mobile apps* for IBA purposes;
- revise your privacy policies to accurately describe how third parties collect and use information on websites *or in mobile apps* for IBA purposes and how users may opt out;
- ensure that you provide ''enhanced notice'' of third-party IBA practices in mobile apps, either prior to download (*e.g.*, in the app store on the application's page), during download, on first opening of the app, or at the time cross-app data is first collected *and* in the app's settings or privacy policy;
- obtain affirmative consent to collect and share precise location data through a mechanism that *specifically* discloses the fact that location data will be passed to third parties for IBA purposes; and
- do not collect or share with third parties information from children under age 13, unless you obtain verifiable parental consent, as required under COPPA.

Mobile app developers also can review the FTC's guidance on providing disclosures in mobile apps. *See* FTC, *Mobile Privacy Disclosures: Building Trust through Transparency*, FTC Staff Report (Feb. 2013). The FTC Staff Report highlights the need to have an easily accessible privacy policy in mobile apps and states that ''app developers should provide just-in-time disclosures and obtain affirmative express consent when collecting sensitive information outside the platform's API, such as financial, health, or children's data, or sharing sensitive data with third parties.'' *Id.* at 23. The FTC Staff Report also recommends that mobile app developers work with third-party advertising partners to understand what information is being collected and used by those third parties. Specifically:

[A]pp developers should improve coordination with ad networks and other third parties that provide services for apps so that the apps can provide truthful disclosures to consumers. It is common for app developers to integrate third-party code to facilitate advertising or analytics within an app with little understanding of what information the third party is collecting and how it is being used. App developers should take responsibility for understanding the function of the code they are utilizing.

Id. at 24. To the extent that mobile app developers integrate third-party software development kits (SDKs) into their apps, they should work with the third parties

   ISSN 1098-5190

to ensure that consumers are provided with appropriate notice of how those third parties may collect, use, and share information through the apps.

Looking Beyond the Horizon

Finally, companies should think broadly about how they comply with privacy best practices for online advertising in other contexts and across platforms. Although the Accountability Program is just beginning enforcement in mobile apps, the FTC staff and self-regulatory groups have already started examining the privacy impacts of other emerging technologies, such as cross-device tracking, non-cookie technologies (for example, statistical IDs), and ''addressable TV'' (using TV viewing behavior to target online advertising). *See, e.g.*, DAA, *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015); NAI, *Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI Code of Conduct* (May 18, 2015); FTC, *Fall Technology Series: Smart TV* (event scheduled for Dec. 7, 2016).

To avoid regulatory scrutiny in these areas, companies should adhere to self-regulatory and FTC guidance and provide an appropriate level of notice and choice for any practices that would be inconsistent with their relationships with consumers.