Reviewing the US data regulators' approach to mobile app privacy

Federal and state regulators in the US are continuing to hone in on mobile device application ('app') privacy issues. As discussed below, the Federal Trade Commission (FTC) recently released new guidelines for mobile app developers, while Kamala D. Harris, the California Attorney General, continued her efforts to enforce the state's online privacy protection law. These actions are a reminder that app developers and their partners should review their app data privacy and security practices and ensure that any apps collecting personal information comply with applicable federal and state laws. Mark W. Brennan, an Associate with Hogan Lovells in Washington D.C, analyses the US regulators' approach in this area, and how companies may start guiding their practices so that they are closer to compliance.

The New FTC Mobile App Privacy Guidelines

On 5 September 2012, the FTC issued a set of truth-in-advertising and privacy guidelines ('the Guidelines') for mobile app developers. Titled 'Marketing Your Mobile App: Get it Right From the Start', the Guidelines provide an overview of key issues for all app developers and other members of the mobile app ecosystem to consider as they engage in the app marketplace[1].

At the outset, the FTC makes clear that the Guidelines are intended to apply to all app developers, large and small, start-up and established. It notes, however, that there is no 'one-size-fits-all' approach to advertising and privacy compliance.

The privacy section of the Guidelines includes several key recommendations:

- build privacy considerations in from the start (i.e., Privacy by Design);
- be transparent about your data practices;
- offer choices that are easy to find and easy to use;
- honor your privacy promises;
- protect kids' privacy;
- collect sensitive information only with consent; and
- keep user data secure.

Privacy

- Build privacy considerations in from the start (i.e., Privacy by Design). The Guidelines recommend that parties incorporate privacy protections into their practices, limit the information they collect, securely store collected information, and dispose of it safely when it is no longer needed. They also encourage parties to select default app settings based on what people using the app would expect. For any collection or sharing of information that is not apparent, the Guidelines state that app developers should obtain express agreement from users.
- Be transparent about your data practices. App developers should 'be clear to users' about their practices and explain what information is collected and how it is used. Interestingly, the Guidelines also reference an expanded disclosure for third party sharing – 'if you share information with another company, tell your users and give them information about that company's data practices'.
- Offer choices that are easy to find and easy to use. The Guidelines state that app developers should provide users with tools to exercise control how their personal information is collected and shared. Such tools should also be easy to find and use, and companies should honor users' choices.
- Honor your privacy promises. App developers must live up to their privacy promises. They also need to obtain affirmative consent to make material changes to their privacy policies. The Guidelines note that such promises should also be made in clear language; easy to read on a small screen; and use colors, fonts, and other design elements to bring attention to key information.
- Protect children's privacy. Apps designed for children or that collect personally identifiable information from children under the age of 13 may have additional requirements under the Children's Online Privacy Protection Act (COPPA) and the FTC's COPPA Rule[2].
- Collect sensitive information only with consent. The Guidelines encourage parties to obtain affirmative consent before collecting 'sensitive' data such as medical, financial, or precise geolocation information.
- Keep user data secure. The Guidelines state that even if parties do not make specific data security promises, they 'still have to take reasonable steps to keep sensitive data secure'. They also recommend that parties: (1) collect only the data they need; (2) secure the data by taking reasonable precautions against well-known security risks; (3) limit access to the data on a need-to-know basis; and (4) safely dispose of data that is no longer needed. App developers that work with contractors and other third parties should 'make sure' that the third parties also comply with these standards.

Truth-in-Advertising

With respect to truth-in-advertising, the Guidelines advise parties to:

● Tell the truth about what your app can do.
● Be transparent about your data practices.

The Guidelines also encourage app developers to look at their product - and their advertising - from 'the perspective of average users, not just software engineers or app experts'. Objective claims need to be backed up with solid proof, also referred to as 'competent and reliable evidence'. Health, safety, or performance claims may need competent and reliable scientific evidence. Disclosures need to be 'big enough and clear enough that users actually notice them and understand what they say'. In other words, avoid burying important terms and conditions.

The California Attorney General's enforcement actions

On 30 October 2012, the Office of California Attorney General Kamala Harris issued a press release[3] confirming that it had begun 'formally notifying' mobile device application operators that they are not in compliance with the California Online Privacy Protection Act of 2003 (CalOPPA). Those companies have 30 days to bring their apps in line with the statute's privacy policy requirements or risk fines of up to $2,500 per app download.

As background, CalOPPA requires operators (i.e., owners) of commercial web sites or online services that collect personally identifiable information (PII) on California residents who use/visit the web sites or online service to 'conspicuously post' a privacy policy. The Attorney General's office has taken the position that mobile apps that use the internet to collect PII are 'online services' subject to CalOPPA. California's population size makes it safe for most app developers to assume that California residents comprise of at least a portion of the app's download audience.

For any collection or sharing of information that is not apparent, the Guidelines state that app developers should obtain express agreement from users

Under the statute, the following information must be included in the privacy policy:
● the categories of PII collected through the app and the categories of third-party persons or entities with whom the operator may share that PII;
● the process by which consumers can review and request changes to any of their PII that was collected through the app, if the operator maintains such a process;
● a description of the process by which the operator notifies app users of material changes to the policy; and
● the effective date of the policy.

The letters are the latest effort by Attorney General Harris to encourage companies to improve the transparency of their data privacy and security practices. In February 2012, she entered into a Joint Statement of Principles[3] agreement with six major app store platforms, setting forth requirements related to app privacy. Facebook later joined the agreement and is now requiring that all apps in its App Center have privacy policies[4].

Mark W. Brennan
Associate
Hogan Lovells
mark.brennan@hoganlovells.com

Footnotes
1.http://business.ftc.gov/documents/bus81-marketing-your-mobile-app
2.15 U.S.C. §§ 6501-6506; 16 C.F.R. Part 312
3.http://oag.ca.gov/news/press_release?id=2630
4.http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer