FTC Publishes Mobile App Advertising and Privacy Do's and Don'ts

Dana B. Rosenfeld, Alysa Z. Hutnik, Gonzalo E. Mon

September 11, 2012

On September 5, 2012, the Federal Trade Commission ("FTC" or "Commission") published a marketing guide[1] for mobile application ("app") developers entitled "Marketing Your Mobile App: Get it Right from the Start" (the "Guide"). In addition to identifying truth-in-advertising standards, the Guide provides basic privacy principles for mobile app developers that align with the core principles contained in the FTC Staff's March 2012 privacy report ("Privacy Report").[2] The key provisions are discussed below.

Truth-In-Advertising Standards

Tell the truth about what your app can do.

The Guide reminds mobile app developers that, once they start distributing their app, they become a marketer. And like all marketers, mobile app developers have a legal responsibility to ensure that their advertising is truthful and not deceptive. Federal law requires that any objective claims—whether on a mobile app developer's website, app store, or within the app—be truthful, not deceptive or unfair, and evidence-based. The Guide provides the following rule of thumb:

Look at your product and your advertising from the perspective of average users, not just software engineers or app experts. If you make objective claims about your app, you need solid proof to back them up before you start selling. The law calls that "competent and reliable evidence."[3]

If a developer is marketing benefits related to health, safety, or performance, the Guide advises that the evidence threshold rises to competent and reliable *scientific* evidence. In pertinent example, last year the FTC settled with marketers over charges in which the FTC claimed the marketers deceptively claimed their mobile apps, AcneApp and Acne Pwner, treated acne with colored lights that emit from smartphones or mobile devices. Click here for a Kelley Drye discussion of this case, as well as two other recent FTC law enforcement actions pertaining to mobile app companies and developers.

Disclose key information clearly and conspicuously.

Federal law requires that advertising disclosures be "clear and conspicuous." As the Guide explains, disclosures must be "big enough and clear enough that users actually notice them and understand what they say." Though the law does not dictate a specific font or type size, the FTC has initiated enforcement actions in the past against companies that have "buried important terms and conditions in long licensing agreements, in dense blocks of legal mumbo jumbo, or behind vague hyperlinks." Mobile app developers should accordingly keep these concepts in mind in determining

where and how to place important disclosures. For a more comprehensive discussion on effective disclosures, read our client advisory on the FTC's May 2012 workshop that explored effective advertising and privacy disclosures in social media and on mobile devices.

Privacy Principles

Build privacy considerations in from the start.

The Guide repeats the familiar FTC adage that companies "bake in" privacy to their practices. For mobile apps, "privacy by design" means (1) incorporating privacy protections into your practice, (2) limiting the information you collect, (3) securely storing what you hold on to, and (4) safely disposing of what you no longer need. The Guide recommends that these principles be applied to the app's default settings. The Guide also urges developers to obtain additional express consent from users for any collection or sharing of information that is either not apparent or inconsistent with users' expectations based on the kind of app being sold. For an expanded discussion of how to incorporate "privacy by design", this Kelley Drye article provides five tips for mobile app developers to stay ahead of the regulators.

Be transparent about your data practices.

The Guide recommends that mobile apps developers be clear to users about their data practices. Specifically, developers should explain what information their apps collect from users or their devices and how the data is being used and shared. In particular, if the information is shared with a third-party, the developer should inform users of the third-party's data collection practices.

Offer choices that are easy to find and easy to use.

The Guide recommends that developers give their users "clear and conspicuous" choice related to privacy settings, opt-outs, and other ways for users to control how their personal information is collected and shared. Specifically, the Guide instructs that developers "[m]ake it easy for people to find the tools you offer, design them so they're simple to use, and follow through by honoring the choices users have made."[4]

Honor your privacy promises.

The Guide recommends that, at a minimum, app developers live up to the promises and representations made in their privacy policies. In recent years, the FTC has brought numerous actions against companies for alleged misrepresentations in their privacy policies about the collection, use, and sharing of consumers' data, and sharing consumers' data without authorization.[5] Additionally, the FTC has opined that developers seeking to materially change the terms of their privacy policy would need to obtain users' affirmative permission. According to the Guide, "just editing the language in your privacy policy isn't enough in those circumstances."

Protect kids' privacy.

The Guide reminds mobile app developers who target children under age 13 of their additional obligations under the Children's Online Privacy Protection Act ("COPPA") and the FTC's COPPA rule ("COPPA Rule"). The COPPA Rule requires website operators to notify parents and obtain their consent before they collect, use, or disclose children's personal information online. The COPPA Rule also requires website operators to post a privacy policy that is clear, understandable, and complete. According to an FTC report on mobile apps for kids released this past February, the majority of children's apps contain almost no information about data collection and sharing practices.[6] The FTC

reported that, in most cases, it wasn't clear whether an app collected any data – let alone what was collected, why it was collected, and who had access. Click here for our coverage of the FTC's first enforcement action in August 2011 for alleged COPPA violations against W3 Innovations, LLC ("W3").

Collect sensitive information only with consent (including precise geolocation data).

The Guide advises that developers should not collect sensitive consumer data, such as medical, financial, or precise geolocation information, without first obtaining users' affirmative consent.

Keep user data secure.

Under federal law, developers must take reasonable steps to keep sensitive data secure. This is true even if developers' privacy policies do not make any promises on how consumers' information will be used. According to the Guide, the wisest policy to protect the data is to:

- Collect only the data you need;
- Secure the data you keep by taking reasonable precautions against well-known security risks;
- Limit access to a need-to-know basis; and
- Safely dispose of data you no longer need.

These principles should be applied both to information received from users and information collected by the developer's software.

* * *

The FTC's guidelines for mobile app developers underscore that the FTC is closely monitoring mobile app practices, particularly with respect to whether app marketers abide by truth-in-advertising laws, privacy principles, and children's privacy requirements. While taking a "privacy by design" approach to mobile apps and carefully vetting all advertising claims requires time and resources, these proactive steps now can help avoid unwanted scrutiny and potential enforcement action by the FTC, as well as state regulators and litigants.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

For more information about this advisory, contact:

Dana B. Rosenfeld
(202) 342-8588
drosenfeld@kelleydrye.com

Alysa Zeltzer Hutnik
(202) 342-8603
ahutnik@kelleydrye.com

Gonzalo E. Mon
(202) 342-8576
gmon@kelleydrye.com

---

[1] Federal Trade Commission, *Marketing Your Mobile App: Get it Right from the Start* (Sept. 2012), https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start ("Guide").
[2] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012), http://ftc.gov/opa/2012/03/privacyframework.shtm ("FTC Privacy Report").
[3] Guide, *supra* note 1, at 1-2.
[4] Guide, *supra* note 1, at 3.
[5] *See, e.g., In re* ScanScout, Inc., FTC No. 1023185 (Nov. 2011), *available at* http://www.ftc.gov/os/caselist/1023185/111108scanscoutagree.pdf (settling claims that ScanScout deceived consumers by advising that Flash cookies could be removed through browser settings); *In re* Google Inc., FTC No. C-4336 (Mar. 2011), available at http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf (settling claims that Google violated its privacy policy when launching Google Buzz); *In re* Chitika, Inc., FTC No. 1023087 (Mar. 2011), *available at* http://www.ftc.gov/os/caselist/1023087/110314chitikaagree.pdf (settling claims that Chitika tracked consumers' online activities even after they opted out of online tracking); *In re* Facebook Inc., FTC No. 092 3184 (Nov. 2011), available at http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf (settling claims that Facebook deceived consumers by failing to keep its privacy promises); In re Myspace LLC, FTC No. 1023058 (May 2012), available at http://www.ftc.gov/os/caselist/1023058/120508myspaceorder.pdf (settling claims that Myspace shared users' profile information with third parties for advertising purposes in violation of its privacy policy).
[6] Federal Trade Commission, *FTC Report Raises Privacy Questions About Mobile Applications for Children* (Feb. 2012), http://ftc.gov/opa/2012/02/mobileapps_kids.shtm.