



February 4, 2013

FTC Releases Recommendations on Mobile Privacy Disclosures**TechComm Client Alert**

This Alert provides only general information and should not be relied upon as legal advice. This Alert may be considered attorney advertising under court and bar rules in certain jurisdictions.

For more information, contact your Patton Boggs LLP attorney or the authors listed below.

Monica Desai
202-457-7535
mdesai@pattonboggs.com

Deborah Lodge
202-457-6030
dlodge@pattonboggs.com

Paul Besozzi
202-457-5292
pbsozzi@pattonboggs.com

Michael Drobac
202-457-7557
mdrobac@pattonboggs.com

Benjamin Bartlett
202-457-7631
bbartlett@pattonboggs.com

Carol Van Cleef
202-457-6435
cvancleef@pattonboggs.com

WWW.PATTONBOGGS.COM

On Friday, February 1, the Federal Trade Commission (FTC) released a staff report recommending best practices for mobile privacy disclosures. The report, available [here](#), reviews the benefits and privacy risks of mobile technologies and recommends ways to inform consumers about data collection and access practices.

The report does not propose rules but provides “recommendations.” Citing the rapid growth in mobile services and users’ growing privacy concerns, the report makes the following recommendations for four categories of industry participants: (1) platforms (i.e., mobile operating systems such as Apple and Google); (2) app developers; (3) third parties such as ad networks; and (4) app trade associations. It also recommends that carriers, handset manufacturers and chip makers review and carefully consider the recommendations.

The FTC strongly encourages companies in the mobile marketplace to implement the report’s recommendations without delay, while it continues to push the envelope in calling out certain information as particularly “sensitive,” in some cases without referencing context. Moreover, the report reflects the FTC’s continuing commitment to monitoring this space.

Mobile platforms should:

- Provide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation
- Consider providing just-in-time disclosures and obtaining affirmative express consent for other content that consumers would find sensitive in many contexts, such as contacts, photos, calendar entries, or the recording of audio or video content
- Consider developing a one-stop “dashboard” approach to allow consumers to review the types of content accessed by the apps they have downloaded
- Consider developing icons to depict the transmission of user data
- Promote app developer best practices such as privacy disclosures
- Consider providing clear disclosures about the extent to which platforms review apps prior to making them available for download in the app stores
- Consider conducting compliance checks after the apps have been placed in the app stores
- Consider offering a Do Not Track (DNT) mechanism for smartphone users

App developers should:

- Have a privacy policy and make sure it is easily accessible through the app stores
- Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information
- Improve coordination and communication with ad networks and other third parties, such as analytics companies, that provide services for apps so the app developers can provide accurate disclosures to consumers
- Consider participating in self-regulatory programs, trade associations and industry organizations, which can provide guidance on how to make uniform, short-form privacy disclosures

Advertising networks and other third parties should:

- Communicate with app developers so that the developers can provide truthful disclosures to consumers
- Work with platforms to ensure effective implementation of DNT for mobile

The FTC expects to issue updated guidance regarding advertising disclosures in a separate report.

App developer trade associations, academics, usability experts and privacy researchers can:

- Develop short form disclosures, such as badges, for app developers
- Promote standardized app developer privacy policies that will enable consumers to compare data practices across apps
- Educate app developers on privacy issues

The FTC's report notes that the National Telecommunications and Information Administration (NTIA) has initiated a multi-stakeholder process to develop a code of conduct on mobile application transparency. The FTC staff report emphasizes that to the extent strong privacy codes are formulated, the agency will view adherence to such codes favorably in connection with its law enforcement work.

Additionally, in conjunction with the release of its recommendations, the FTC introduced a new business guide, titled *Mobile App Developers: Start with Security*, which provides tips intended to help app developers approach mobile data security. A copy of this guide is available [here](#).

As reflected in the FTC's report, the mobile marketplace, as well as the laws and regulations governing it, continue to rapidly evolve. If you have questions or concerns regarding the FTC's report or mobile privacy regulations in general, please contact us.

FTC Chairman Announces Departure

Jon Leibowitz, chairman of the FTC, has announced that he plans to depart the agency around Friday, February 15. Until the Senate confirms a successor to Leibowitz, the chairman's departure will leave a 2-2 split at the five-member commission, potentially limiting some actions at the FTC until a majority is restored. As Chairman Leibowitz spearheaded many of the recent FTC agenda items, including mobile privacy, the change in leadership may result in some shift in priorities. Privacy, however, is likely to remain high on the list of his successor.

This Alert provides only general information and should not be relied upon as legal advice. This Alert may also be considered attorney advertising under court and bar rules in certain jurisdictions.

WASHINGTON DC | NEW JERSEY | NEW YORK | DALLAS | DENVER | ANCHORAGE | DOHA | ABU DHABI | RIYADH