

FTC ISSUES MOBILE PRIVACY AND SECURITY PUBLICATIONS

On February 1, 2013, the Federal Trade Commission (FTC) issued two publications recommending ways that key players in the mobile marketplace, such as operating system providers, application developers, advertising networks and analytics companies, can promote mobile privacy and security.

The first publication, titled "[Mobile Privacy Disclosures: Building Trust Through Transparency](#)," recommends ways to inform consumers about data collection and use practices.

Recommendations for operating systems providers include:

- Providing just-in-time disclosures and obtaining affirmative express consent before allowing apps to access consumers' sensitive content;
- Considering a one-stop "dashboard" approach to allow consumer review of the types of content accessed by downloaded apps;
- Considering icons to depict the transmission of user data;
- Promoting app developer best practices, such as privacy disclosures; and
- Considering a Do Not Track (DNT) mechanism for smartphone users.

App developers should:

- Have an easily accessible privacy policy;
- 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 that provide services for apps; and
- Consider participating in self-regulatory programs, trade associations and industry organizations.

The FTC also published "[Mobile App Developers: Start with Security](#)." In the guide, the agency says it expects mobile application developers to adopt and maintain reasonable data security practices but recognizes there is no one checklist for securing all apps. Tips for mobile app security offered by the agency include:

- Make someone responsible for security;
- Take stock of the data collected and retained;
- Understand differences between mobile platforms;
- Don't rely on a platform alone to protect users;
- Generate credentials securely;
- Use transit encryption for usernames, passwords and other important data;
- Use due diligence on libraries and other third-party code;
- Consider protecting data stored on a user's device;
- Protect servers;
- Don't store passwords in plaintext; and
- Understand applicable standards and regulations when dealing with financial, health or kids' data.

If you have questions about privacy and security practices for mobile devices and other health information technology products, please contact Jeffrey W. Short at jshort@hallrender.com (317-977-1413), Mark T. Garsombke at mgarsombke@hallrender.com (414-721-0907), Melissa L. Markey at mmarkey@hallrender.com (248-457-7853) or Mark R. Dahlby at mdahlby@hallrender.com (414-721-0902).