Taming the Wild West: FTC Report Urges Mobile App Industry to Adopt Strong Privacy Measures

Karen H Bromberg, Partner

App providers and developers are in the hot seat again. On the same day that the FTC fined the social networking app Path $800,000 over allegations that it collected personal information without obtaining consumers' consent, the FTC released a report outlining privacy guidelines for mobile platform providers, application developers, and advertising networks (the "Report"). Explaining the Commission's increased attention to this area, the outgoing FTC Commissioner described the current state of rules and practices in the mobile space as a sort of "Wild West." Cautioning that the Commission will "closely monitor developments in this space", the FTC "strongly" encouraged companies in the mobile ecosystem to work expeditiously to implement the recommendations in the Report. The guidance focuses on how mobile app players should improve their disclosures to ensure that users understand how their personal data will be collected and used.

While the FTC guidelines are directed to all players in the mobile arena, the Report emphasizes that platform providers (such as Amazon, Apple, Blackberry, Google, and Microsoft), are "the gatekeepers to the app marketplace", and thus have the greatest ability to effect improvements to mobile privacy disclosure. The Report suggests that platform providers and developers build in privacy protection at every stage in developing their products, provide consumers with choices related to privacy at the relevant time and in the relevant context, and disclose details about their collection and use of consumers' information.

Among the specific recommendations, the Report suggests that platform providers consider "offering a Do Not Track (DNT) mechanism for smartphone users," and that they create a "dashboard" for consumers. The dashboard feature would allow users to see the content being accessed by the apps they have downloaded. The Report also urges platforms providers to develop icons to be displayed when user data is transmitted, and to provide "just-in-time disclosures" to consumers, which would require consumers to provide express consent before an app accesses potentially sensitive information. To the extent that the platform providers do not obtain user consent before accessing sensitive user information, the Report encourages app developers to do so.

With respect to app developers, the Report stresses that they maintain an easily accessible privacy policy available through their app stores and work to improve their coordination with companies providing services for apps, such as advertising networks and companies that provide analytics, to ensure that accurate disclosures are provided to the end user. The Report further advises app developers to consider participating in various industry and trade groups to facilitate providing uniform short-form

privacy disclosure statements in order to allow consumers to compare privacy practices of different apps akin to reviewing nutrition labels on food.

The Report recommends that advertising networks and other third parties communicate with app developers to help them provide accurate disclosures, and assist platform providers so that they can provide effective implementation of DNT mechanisms for mobile devices.

Although the Report is not binding, it is an indication of how seriously the agency is focused on mobile privacy. While following the guidelines may not immunize a company from liability, it provides a road map of what kinds of activities might render it the target of an investigation – such as, for example, conveying the impression that an app gathers geolocation data only once, when, in truth, it does so repeatedly.

The FTC also posted on its Bureau of Consumer Protection Business Center website new data security guidance for mobile apps developers. This security guidance advises developers to implement "reasonable data security" in the development stage of an app and offers a checklist of measures that developers should consider to ensure the privacy and security of their users' data.

The full Report can be viewed here.

About the Author

Ms. Bromberg is the head of the firm's Intellectual Property and Licensing Group. She handles all aspects of intellectual property, Internet, and technology law, including license agreements, technology transfer and vendor agreements, joint development and co-branding agreements, privacy policies, website terms of service, and management of IP litigation (including patent, trademark, copyright, and trade secret litigation). She was named as a New York *Super Lawyer* for Intellectual Property in 2010, 2011, and 2012.

About Cohen & Gresser

Cohen & Gresser is a boutique law firm with offices in New York and Seoul. We represent clients in complex litigation and corporate transactions throughout the world. Founded in 2002, the firm has grown to over fifty lawyers in four practice groups: Litigation and Arbitration; Corporate Law; Intellectual Property and Licensing; and White Collar Defense, Regulatory Enforcement and Internal Investigations. Our attorneys are graduates of the nation's best law schools and have exceptional credentials. We are committed to providing the efficiency and personal service of a boutique firm and the superb quality and attention to detail that are hallmarks of the top firms where we received our training.

NEW YORK | SEOUL

www.cohengresser.com info@cohengresser.com PH: +1 212 957 7600