FTC on the Move: Mobile Enforcement and Policy Recommendations Demonstrate Heightened Interest in Mobile Privacy Issues

by Mary Ellen Callahan, David M. Didion, and Sabrina N. Guenther

This month, the Federal Trade Commission (FTC) has redoubled its mobile privacy enforcement and policy efforts, with the specter of additional enforcement actions anticipated in the near future.

On February 22, 2013, the FTC announced its first Consent Order agreement for alleged unfair and deceptive trade practices against a mobile device manufacturer, HTC America, Inc. (HTC), maker of Android-based mobile devices. This Consent Order is noteworthy for several reasons: first, the definition of covered information is very broad, including “individually identifiable information” such as precise geolocation, static IP address, MAC address, cookies, and almost all information on a particular mobile device; second, the FTC is continuing its pursuit of legal theories against “unfair” data security practices whenever it perceives a security gap; and third, although this Consent Order involves a mobile device manufacturer, the conclusions and content could be applied to many participants in the mobile industry.

No Security Standards or Programs

The FTC charged HTC with three counts, but the bulk of the FTC’s complaint focused on count one, HTC’s alleged failure to employ reasonable security measures to protect sensitive information in its mobile devices. Specifically, the FTC alleged that HTC employed security practices so lax as to be unfair to consumers, including:

(a) failing to implement an adequate program to assess the security of products it shipped to consumers; (b) failing to implement adequate privacy and security guidance or training for its engineering staff; (c) failing to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices; (d) failing to follow well-known and commonly accepted secure programming practices, including secure practices that were expressly described in the operating system’s guides for manufacturers and developers, which would have ensured that applications only had access to users’ information with their consent; and (e) failing to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.

In counts two and three, the FTC also alleged that HTC had deceptively misrepresented its permissions-based security system and had misrepresented the location information provided to HTC through a consumer’s error report.

The terms of the Consent Order continue the FTC’s emphasis on implementing prevention measures and
adequate information security protocols, rather than just remedying the specific software inadequacies alleged in the FTC’s complaint. Under the Consent Order, HTC must, among other remedies, implement a comprehensive written security program designed to address security risks related to HTC’s new and existing covered devices and to protect the security, confidentiality, and integrity of information collected by HTC or input into, stored on, captured with, accessed or transmitted through a covered device. In addition, HTC must provide security patches to fix the specific vulnerabilities identified in the FTC’s complaint. However, the Consent Order explicitly does not require HTC to identify and correct security vulnerabilities in third parties’ software on covered devices to the extent the vulnerabilities are not the result of HTC’s integration, modification, or customization of the third-party software.

Information at Risk

The FTC’s complaint and the Consent Order also offer new insight into the scope of potentially sensitive mobile data, which could have significant implications for any company operating within mobile platforms. The Consent Order defines “covered information” as:

- individually-identifiable information from or about an individual consumer collected by respondent through a covered device or input into, stored on, captured with, or transmitted through a covered device, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (IP) address, a mobile device ID, or processor serial number; (j) precise geolocation data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; (k) an authentication credential, such as a username and password; or (l) any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, emails, text messages, photos, videos, and audio recordings.

Notably, several of these categories extend beyond traditionally protected categories of information, which often include first and last names, email and street addresses, telephone numbers, or other personally identifiable information. In particular, the catch-all category in item (l) could extend to almost all information on a particular mobile device, and the persistent identifiers in item (i) and screen names in item (c) are new extensions of the definitions of protected information outside of the COPPA context. Thus, the FTC has created a much broader definition of protected information, to the detriment of the mobile industry.

The proposed resolution of the FTC’s first case against a mobile device maker underscores the FTC’s mounting interest in the privacy and security of a broad range of mobile data. The Consent Order offers insight into best security practices for companies in the mobile industry. Those companies should look to the detailed requirements for HTC’s information security program and the broad definition of information covered by the program as a guide to evaluate their own security practices.

FTC Report on Mobile Disclosures

Earlier this month, on February 1, 2013, the FTC foreshadowed some of these mobile enforcement trends when it released a set of best practice recommendations—Mobile Privacy Disclosures: Building Trust through Transparency—targeted at platforms, app developers, third parties (such as ad networks and analytics companies), and app trade associations, and released a Consent Order against a mobile social network for alleged COPPA and deceptive trade practice violations.

These FTC mobile recommendations mostly focus on disclosure. They have a narrower scope and are not as prescriptive as the January 2013 California AG (CA AG) guidelines—for example, they have no encryption or deletion requirements. The recommendations extend beyond the current law, but—especially where they overlap with the CA AG’s guidelines—they may set a new baseline for potential exposure to enforcement actions. The HTC Consent Order now casts some of these recommendations in a clearer light.

Specifically, the FTC recommends the following privacy practices for app developers:
• Notice via Privacy Policy: App developers should have a privacy policy and make sure it is easily accessible through the app stores.
  o The CA AG also requires a privacy policy and requires making that privacy policy accessible before download.

• Just-in-Time Notices and Consent for Sensitive Data Collection and Sharing: App developers should provide just-in-time disclosures and obtain affirmative express consent before collecting or sharing with third parties sensitive information such as financial, health, or children’s data.
  o The recommendations also specify that platform providers should issue just-in-time disclosures (and seek user consent) when apps access “sensitive” content such as geolocation information, photos, contacts, calendar entries, or the recording of audio or video content.
  • App developer disclosures should not overlap with platform disclosures. This may require platform/developer coordination.
  o The recommendations do not define terms, but it may be reasonable to assume that, for example, sensitive geolocation corresponds to the definition the FTC adopted in COPPA—namely, geolocation at the city and street level.
  o Though the guidelines do not define sensitive information, the FTC's complaint against HTC might provide a hint at its scope when that complaint alleged “insecure communications mechanisms” exposed “sensitive information,” a broad category that includes “GPS-based location information; web browsing and media viewing history; the size and number of all text messages; the content of each incoming text message; the names of applications on the user’s device; the numeric keys pressed by the user; and any other usage and device information specified for collection by certain network operators."

• Understanding Third-Party Data Access and Code: App developers need to 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.
  o The FTC seems to be signaling here that it will hold app developers more accountable when those developers integrate third-party code—which may facilitate advertising or analytics within an app—with little understanding of what information the third party is collecting and how it is being used.

The FTC also introduced the concept of a “do not track” for mobile devices, which is the first time it has suggested such a practice for mobile devices. To the extent that individual app developers use third-party ad serving or analytics, there may need to be structural changes to that process in the mid-term future.

App developers should proactively review their data collection and use practices within their apps; in addition, they should review whether the privacy policy is disclosed in the app store (a threshold question). The FTC’s focus on understanding third-party activities heightens the need to know what happens within an application. Third-party relationships and geolocation are two areas of highest sensitivity following the FTC report, together with the issues highlighted in the more recent HTC Consent Order. In particular, app developers should be alert that the FTC is growing more openly concerned about the types of data included in the complaint and Consent Order’s “sensitive” and “covered” information categories, and that the FTC continues to pursue “unfair” data practices where it perceives a security gap.

For further information, please contact:

**Mary Ellen Callahan**
Partner  
Tel: 202 639-6064  
Email: mecallahan@jenner.com

**David M. Didion**
Associate  
Tel: 202 639-6082  
Email: ddidion@jenner.com

**Sabrina N. Guenther**
Associate  
Tel: 312 840-7299  
Email: sguenther@jenner.com