FTC Finds HTC Mobile Devices Fail to Protect Personal Data

Mobile devices made by HTC America, Inc. contain serious security flaws, which allow the phones to send their own text messages, send personally identifiable information to third parties, and even activate the microphone to listen to conversations, according to a proposed consent decree with the Federal Trade Commission (FTC).

The FTC's complaint noted that HTC's security flaws potentially expose the user's sensitive information, making consumers "at risk of financial and physical injury and other harm." The FTC said HTC failed:

- To implement an adequate program to assess the security of products it shipped to consumers;
- To implement adequate privacy and security guidance or training for its engineering staff;
- To conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices;
- To follow well-known and commonly-accepted secure programming practices, including practices which were expressly described in the operating system's guides; and
- To implement a process for receiving and addressing security vulnerability reports from third party researchers.

HTC develops and manufactures smartphones and tablet computers using Google, Inc.'s Android operating system and Microsoft Corp.'s Windows Mobile and Windows Phone mobile operating systems.

As a result of HTC's failures, tens of millions of HTC devices were open to third-party exploitation. "Sensitive information exposed on these devices could be used, for example, to target spear-phishing campaigns, physically track or stalk individuals, and perpetrate fraud, resulting in costly bills to the consumer."

For example, HTC allowed any third party access to the device's microphone without the owner's permission, so that a third party could listen and record conversations, which "allow[s] hackers to capture private details of an individual's life," the complaint found. Third parties also could gain access to the device's texting function, allowing "toll fraud," that is, sending text messages to premium numbers in order to charge fees to the owner's phone bill.

"Because the communications mechanisms were insecure, any third-party application that could connect to the internet could communicate with the logging applications on HTC devices and access a variety of sensitive information and sensitive device functionality," the FTC complaint states. The information that could be accessed included:

- Contents of text messages;
- Last known location and a limited history of GPS locations;

- A user's personal phone number;
- Mobile equipment identification numbers;
- Account user names; and
- Web browsing history.

Under the settlement, HTC agreed to issue patches for the security lapses, to establish a comprehensive program to address security risks, and to notify customers about the security vulnerabilities.

The public has until March 22, 2013 to file comments with the FTC regarding the consent decree.

In the Matter of HTC America, Inc., FTC File No. 122 3049