122 3049

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
Edith Ramirez
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

	)	
In the Matter of	)	**DOCKET NO. C-**
	)	
HTC AMERICA Inc.,	)	
a corporation.	)	
	)	
	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that HTC America, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent HTC America Inc. ("HTC") is a Washington corporation with its principal office or place of business at 13920 SE Eastgate Way, Suite #400, Bellevue, WA 98005.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

3. Respondent is a mobile device manufacturer that develops and manufactures smartphones and tablet computers using Google Inc.'s ("Google") Android operating system and Microsoft Corporation's ("Microsoft") Windows Mobile and Windows Phone mobile operating systems.

ANDROID'S PERMISSION-BASED SECURITY MODEL

4. Google's Android operating system protects certain sensitive information (e.g., location information or the contents of text messages) and sensitive device functionality (e.g., the ability to record audio through the device's microphone or the ability to take photos with the device's camera) through a permission-based security model. In order to access sensitive information or sensitive device functionality, a third-party application must declare the fact that it will access such information or functionality.

5. Before a user installs a third-party application, the Android operating system provides notice to the user regarding what sensitive information or sensitive device functionality the application has declared it requires. The user must accept these “permissions” in order to complete installation of the third-party application.

HTC’S FAILURE TO EMPLOY REASONABLE SECURITY IN THE CUSTOMIZATION OF ITS MOBILE DEVICES

6. HTC has customized its Android-based mobile devices by adding and/or modifying various pre-installed applications and components in order to differentiate its products from those of competitors also manufacturing Android-based mobile devices. HTC has also customized both its Android and Windows Mobile devices in order to comply with the requirements of certain network operators, such as Sprint Nextel Corporation (“Sprint”) and AT&T Mobility LLC (“AT&T”). Since the customized applications and components are pre-installed on the device, consumers do not choose to install the customized applications and components, and the device user interface does not provide consumers with an option to uninstall or remove the customized applications and components from the device.

7. Until at least November 2011, respondent engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices. Among other things, respondent: (a) failed to implement an adequate program to assess the security of products it shipped to consumers; (b) failed to implement adequate privacy and security guidance or training for its engineering staff; (c) failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices; (d) failed 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) failed 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.

8. As a result of its failures described in Paragraph 7, HTC introduced numerous security vulnerabilities in the process of customizing its mobile devices. Once in place, HTC failed to detect and mitigate these vulnerabilities, which, if exploited, provide third-party applications with unauthorized access to sensitive information and sensitive device functionality. The following examples in paragraphs 9 to 15 serve to illustrate the consequences of HTC’s failure to employ reasonable and appropriate security in the design and customization of the software on its mobile devices.

PERMISSION RE-DELEGATION

9. HTC undermined the Android operating system’s permission-based security model in its devices by introducing numerous “permission re-delegation” vulnerabilities through its custom, pre-installed applications. Permission re-delegation occurs when one application

that has permission to access sensitive information or sensitive device functionality provides another application that has not been given the same level of permission with access to that information or functionality. For example, under the Android operating system's security framework, a third-party application must receive the user's permission to access the device's microphone, since the ability to record audio is considered sensitive functionality. But in its devices, HTC pre-installed a custom voice recorder application that, if exploited, would provide any third-party application access to the device's microphone, even if the third-party application had not requested permission for that functionality.

10. HTC could have prevented this by including simple, well-documented software code - "permission check" code - in its voice recorder application to check that the third-party application had requested the necessary permission. Because HTC failed in numerous instances to include permission check code in its custom, pre-installed applications, any third-party application exploiting these vulnerabilities could command those HTC applications to access various sensitive information and sensitive device functionality on its behalf -- including enabling the device's microphone; accessing the user's GPS-based, cell-based, and WiFi-based location information; and sending text messages -- all without requesting the user's permission.

11. Malware could exploit these vulnerabilities to, for example, surreptitiously record phone conversations or other sensitive audio, to surreptitiously track a user's physical location, and to perpetrate "toll fraud," the practice of sending text messages to premium numbers in order to charge fees to the user's phone bill. These vulnerabilities have been present on approximately 18.3 million HTC devices running Android v. 2.1.x, 2.2.x, 2.3.x, and 3.0.x.

APPLICATION INSTALLATION VULNERABILITY

12. Relatedly, HTC pre-installed a custom application on its Android-based devices that could download and install applications outside of the normal Android installation process. Again, HTC failed to include appropriate permission check code to protect this pre-installed application from exploitation. As a result, any third-party application exploiting the vulnerability could command this pre-installed application to download and install any additional applications from any server onto the device without the user's knowledge or consent. Because this would occur outside the normal installation process, the user would not be presented with a permission screen that explained what sensitive information or sensitive device functionality the additional application being installed would be able to access. In effect, this vulnerability undermines all protections provided by Android's permission-based security model. This vulnerability has been present on approximately 18.3 million HTC devices running Android v. 2.1.x, 2.2.x, 2.3.x, 3.0.x and certain devices that were upgraded to Android v. 4.0.x.

INSECURE COMMUNICATIONS MECHANISMS

13. HTC failed to use readily-available and documented secure communications mechanisms in implementing logging applications on its devices, placing sensitive information at risk.

Logging applications collect information that can be used, for example, to diagnose device or network problems. Because of the sensitivity of the information, as described below, communications with logging applications should be secure to ensure that only designated applications can access the information. Secure communications mechanisms -- such as the Android inter-process communication mechanisms expressly described in the Android developer guides, or secure UNIX sockets – could have been used to ensure that only HTC-designated applications could access the sensitive information collected by the logging application. Instead of using one of these well-known, secure alternatives, HTC implemented communication mechanisms (e.g., INET sockets) that could not be restricted in a similar manner. Moreover, HTC failed to implement other, additional security measures (e.g., data encryption) that could have secured these communications mechanisms. 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, as described below.

a. HTC Loggers. Beginning in May 2010, HTC installed its customer support and trouble-shooting tool HTC Loggers on approximately 12.5 million Android-based mobile devices. Because HTC Loggers could collect sensitive information from various device logs, it was supposed to have been accessible only to HTC and certain network operators, and only after the user had consented to its use by manually entering a special code into the mobile device. Moreover, the Android permission-based security model normally requires a third-party application to obtain the user's consent before accessing the device logs. Because HTC used an insecure communications mechanism, however, both of these intended protections were undermined, and any third-party application on the user's device that could connect to the internet could exploit the vulnerability to communicate with HTC Loggers without authorization and command it to collect and transmit information from the device logs. This information could include, but was not limited to, contents of text messages; last known location and a limited history of GPS and network locations; a user's personal phone number, phone numbers of contacts, and phone numbers of those who send text messages to the user; dialed digits; web browsing and media viewing history; International Mobile Equipment Identity ("IMEI") or Mobile Equipment Identifier ("MEID"); and registered accounts such as Gmail and Microsoft Exchange account user names.

b. Carrier IQ. Beginning in 2009, HTC embedded Carrier IQ diagnostics software on approximately 10.3 million Android-based mobile devices and 330,000 Windows Mobile-based mobile devices at the direction of network operators Sprint and AT&T, who used Carrier IQ to collect a variety of information, described in subparagraph (i) below, from user devices to analyze network and device problems. In order to embed the Carrier IQ software on its mobile devices, HTC developed a "CIQ Interface" that would pass the necessary information to the Carrier IQ software. The information collected by the Carrier IQ software was supposed to have been accessible only to the network operators, but because HTC used an insecure communications mechanism, any third-party application on the user's device that could connect to the internet could exploit the vulnerability to communicate with the CIQ Interface, allowing it to:

i. Intercept the sensitive information being collected by the Carrier IQ software. This information could include, but was not limited to, 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; and

ii. In the case of HTC's Android-based devices, perform potentially malicious actions, including, but not limited to, sending text messages without permission. As described in Paragraph 11, malware could exploit this vulnerability to perpetrate toll fraud. Moreover, in this case, the sent text messages would not appear in the user's outbox, making it impossible for the user to verify that unauthorized text messages had been sent from the device.

DEBUG CODE

14. During the development of an application, developers may activate "debug code" in order to help test whether the application is functioning as intended. When developing its CIQ Interface for its Android-based devices, HTC activated debug code in order to test whether the CIQ Interface properly sent all of the information specified by the network operator. The debug code accomplished this by writing the information to a particular device log known as the Android system log, which could then be reviewed. However, HTC failed to deactivate the debug code before its devices shipped for sale to consumers. As a result of the active debug code, all information that the CIQ Interface sent to the Carrier IQ software from a consumer's device, including the information specified in Paragraph 13(b)(i), was also written to the Android system log on the device. This information was supposed to have been accessible only to the network operators, never written to the system log. Because it ended up in the system log, this sensitive information was:

a. Accessible to any third-party application with permission to read the system log. Although users may provide third-party applications with permission to read the system log for certain purposes -- for example, to trouble-shoot application crashes -- those applications never should have had access to all the sensitive information, such as the contents of incoming text messages, that the Carrier IQ software was collecting.

b. Sent to HTC. The information in the system log is sent to HTC when a user chooses to send HTC an error report through its "Tell HTC" error reporting tool, described in Paragraph 20. Accordingly, in some cases, HTC also received this sensitive information, including users' GPS-based location information.

15. HTC could have detected its failure to deactivate the debug code in its CIQ Interface had it had adequate processes and tools in place for reviewing and testing the security of its software code.

CONSUMERS RISK HARM DUE TO HTC'S SECURITY FAILURES

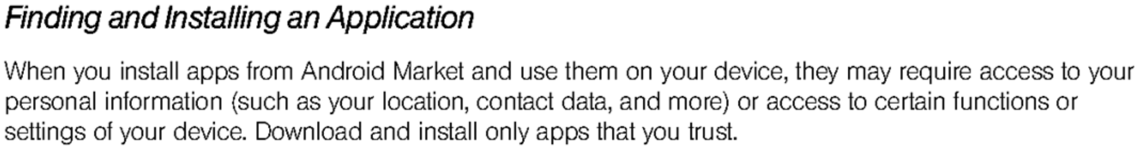
16. Because of the potential exposure of sensitive information and sensitive device functionality through the security vulnerabilities in HTC mobile devices, consumers are at risk of financial and physical injury and other harm. Among other things, malware placed on consumers' devices without their permission could be used to record and transmit information entered into or stored on the device, including financial account numbers and related access codes or personal identification numbers, medical information, and personal information such as text messages and photos. Sensitive information exposed on the 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. Misuse of sensitive device functionality such as the device's audio recording feature would allow hackers to capture private details of an individual's life.

17. In fact, malware developers have targeted the types of sensitive information and sensitive device functionalities that potentially are exposed through the security vulnerabilities in HTC mobile devices. Text message toll fraud, for example, is one of the most common types of Android malware. Security researchers have also found Android malware that records and stores users' phone conversations and that tracks users' physical location.

18. Had HTC implemented an adequate security program, it likely would have prevented, or at least timely resolved, many of the serious security vulnerabilities it introduced through the process of customizing its mobile devices. HTC could have implemented readily-available, low-cost measures to address these vulnerabilities – for example, adding a few lines of permission check code when programming its pre-installed applications, or implementing its logging applications with secure communications mechanisms. Consumers had little, if any, reason to know their information was at risk because of the vulnerabilities introduced by HTC.

HTC'S PRIVACY AND SECURITY REPRESENTATIONS

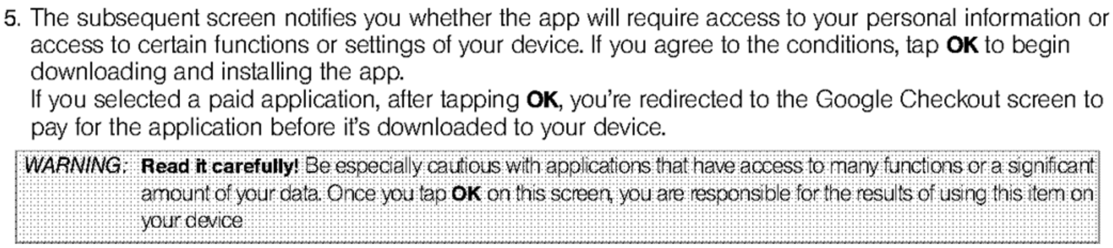
19. Since at least October 2009, user manuals for HTC's Android-based mobile devices contained the following statements, or similar statements, regarding Android's permission-based security model:



Finding and Installing an Application

When you install apps from Android Market and use them on your device, they may require access to your personal information (such as your location, contact data, and more) or access to certain functions or settings of your device. Download and install only apps that you trust.

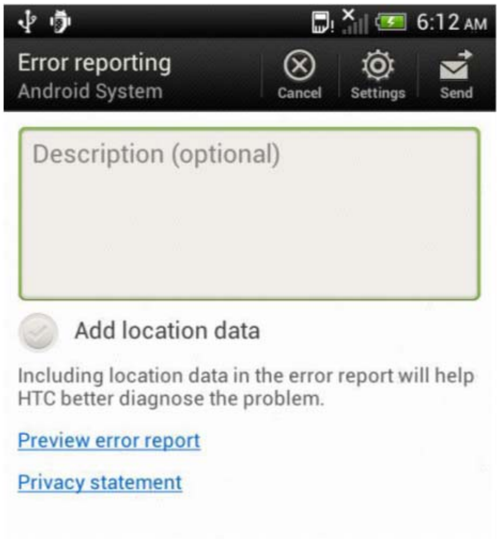
. . .



5. The subsequent screen notifies you whether the app will require access to your personal information or access to certain functions or settings of your device. If you agree to the conditions, tap **OK** to begin downloading and installing the app.
If you selected a paid application, after tapping **OK**, you're redirected to the Google Checkout screen to pay for the application before it's downloaded to your device.

WARNING: **Read it carefully!** Be especially cautious with applications that have access to many functions or a significant amount of your data. Once you tap **OK** on this screen, you are responsible for the results of using this item on your device

20. Since at least June 2011, HTC has, in many of its Android-based mobile devices, included the Tell HTC error reporting tool. The error reporting tool provides the user with an opportunity to send a report to HTC when there is an application or system crash. The report includes the information in the Android system log. The Tell HTC user interface provides the user with the additional option of submitting location information with the report by checking the button marked "Add location data," as depicted below:



Description (optional)

○ Add location data

Including location data in the error report will help HTC better diagnose the problem.

Preview error report

Privacy statement

Through this user interface, HTC represents that the user's location data will not be sent to HTC if the user does not check the button marked "Add location data."

HTC'S UNFAIR SECURITY PRACTICES
(Count 1)

21. As set forth in Paragraph 7-18, HTC failed to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices. HTC's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

HTC'S DECEPTIVE ANDROID USER MANUALS
(Count 2)

22. As described in Paragraph 19, HTC has represented, expressly or by implication, that, through the Android permission-based security model, a user of an HTC Android-based mobile device would be notified when a third-party application required access to the user's personal information or to certain functions or settings of the user's device before the user completes installation of the third-party application.

23. In truth and in fact, in many instances, a user of an HTC Android-based mobile device would not be notified when a third-party application required access to the user's personal information or to certain functions or settings of the user's device before the user completes installation of the third-party application. Due to the security vulnerabilities described in Paragraphs 8-15, third-party applications could access a variety of sensitive information and sensitive device functionality on HTC Android-based mobile devices without notifying or obtaining consent from the user before installation. Therefore, the representation set forth in Paragraph 22 constitutes a false or misleading representation.

HTC'S DECEPTIVE TELL HTC USER INTERFACE
(Count 3)

24. As described in Paragraph 20, HTC has represented, expressly or by implication, that, if a user does not check the button marked "Add location data" when submitting an error report through the Tell HTC application, location data would not be sent to HTC with the user's error report.

25. In truth and in fact, in some instances, if a user did not check the button marked "Add location data" when submitting an error report through the Tell HTC application, location data was nevertheless sent to HTC with the user's error report. Due to the security vulnerability described in Paragraph 14, in some instances, HTC collected the user's GPS-based location information through the Tell HTC error reporting tool even when the user had not checked the button marked "Add location data" in the Tell HTC user interface. Therefore, the representation set forth in Paragraph 24 constitutes a false or misleading representation.

26. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this ___ day of __________, 2013, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary