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'

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.

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 appa t i s a s

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

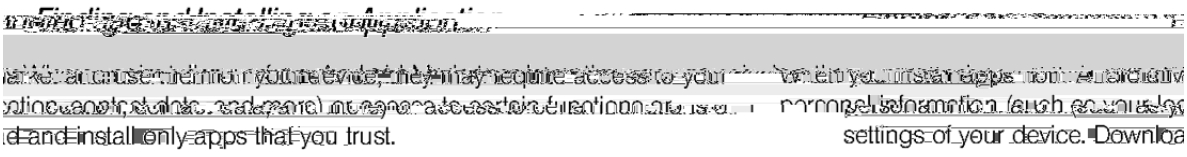
16. Because of the potential exposure of sensitive information and sensitive device functionality through the security vulnerabilities in HTC mobile devices, consumers are at risk of financial and physical injury and other harm. Among other things, malware placed on consumers' devices without their permission 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.

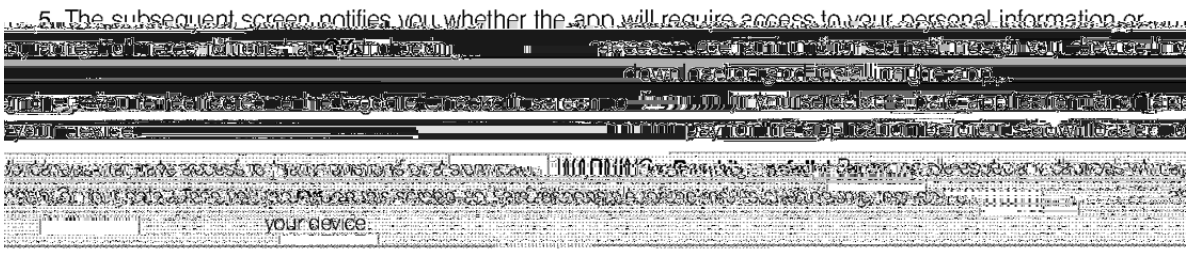
18. Had HTC implemented an adequate security program, it likely would have prevented, or at least timely resolved, many of the serious security vulnerabilities it introduced through the process of customizing its mobile devices. HTC could have implemented readily-available, low-cost measures to address 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

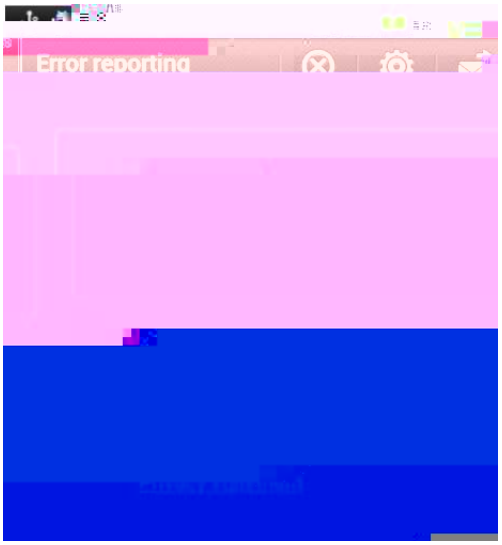
19. Since at least October 2009, user manuals for HTC's Android-based mobile devices contained the following statements, or similar statements, regarding Android's permission-based security model:



. . .



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:



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