Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of HTC America, Inc., File No. 122 3049

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to HTC America, Inc. ("HTC").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

HTC is a mobile device manufacturer that develops and manufactures smartphones and tablet computers using Google Inc.'s Android operating system and Microsoft Corporation's Windows Mobile and Windows Phone operating systems. HTC has customized its Android-based mobile devices by adding 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. As 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.

The Commission's complaint alleges that HTC engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security in the design and customization of software on its mobile devices. Among other things, HTC:

(1) failed to implement an adequate program to assess the security of products it shipped to consumers;

(2) failed to implement adequate privacy and security guidance or training for its engineering staff;

(3) failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices;

(4) 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;

(5) 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.

The complaint further alleges that, due to these failures, 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 sensitive device functionality potentially exposed by the vulnerabilities includes the ability to send text messages without permission, the ability to record audio with the device's microphone without permission, and the ability to install other applications, including malware, onto the device without the user's knowledge or consent. The complaint alleges that 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, and medical information. In addition, other sensitive information exposed by the vulnerabilities includes, but is not limited to, location information, the contents of text messages, the user's personal phone number, phone numbers of contacts, phone numbers of those who send text messages to the user, and the user's web and media viewing history.

The proposed order contains provisions designed to prevent HTC from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits HTC from misrepresenting the extent to which HTC or its products or services -- including any covered device -- use, maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of covered information from or about consumers. Part II of the proposed order requires HTC to (1) address security risks related to the development and management of new and existing covered devices, and (2) protect the security, confidentiality, and integrity of covered information, whether collected by respondent or input into, stored on, captured with, accessed or transmitted through a covered device. The security program must contain administrative, technical, and physical safeguards appropriate to HTC's size and complexity, nature and scope of its activities, and the sensitivity of the information collected from or about consumers. Specifically, the proposed order requires HTC to:

- designate an employee or employees to coordinate and be accountable for the information security program;

- identify material internal and external risks to the security of covered devices that could result in unauthorized access to or use of covered device functionality, and assess the sufficiency of any safeguards in place to control these risks;

- identify material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in HTC's possession or is input into, stored on,

captured with, accessed or transmitted through a covered device, and assess the sufficiency of any safeguards in place to control these risks;

- consider risks in each area of relevant operation, including but not limited to (1) employee training and management; (2) product design, development and research; (3) secure software design and testing, including secure engineering and defensive programming; and (4) review, assessment, and response to third-party security vulnerability reports;

- design and implement reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security testing techniques, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

- develop and use reasonable steps to select and retain service providers capable of maintaining security practices consistent with the order, and require service providers by contract to implement and maintain appropriate safeguards; and

- evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to HTC's operations or business arrangement, or any other circumstances that it knows or has reason to know may have a material impact on its security program.

However, Part II 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 respondent's integration, modification, or customization of the third party software.

Part III of the proposed order requires HTC to develop security patches to fix the security vulnerabilities in each affected covered device having an operating system version released on or after December 2010. Within thirty (30) days of service of the order, HTC must release the security patches either directly to affected covered devices or to the applicable network operator for deployment to the affected covered devices. HTC must provide users of the affected covered devices with clear and prominent notice regarding the availability of the security patches and instructions for installing the security patches.

Part IV of the proposed order requires HTC to obtain, within the first one hundred eighty (180) days after service of the order and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security of covered device functionality and the security, confidentiality, and integrity of covered information is protected.

Parts V through IX of the proposed order are reporting and compliance provisions. Part V requires HTC to retain documents relating to its compliance with the order. The order requires that the documents be retained for a three-year period. Part VI requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. Part VII ensures notification to the FTC of changes in corporate status. Part VIII mandates that HTC submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part IX is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint or order or to modify the order's terms in any way.