

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

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

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.