UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	**AGREEMENT CONTAINING CONSENT ORDER**
	)	
HTC America Inc., **a corporation.**	)	
	)	**FILE NO. 122 3049**

The Federal Trade Commission has conducted an investigation of certain acts and practices of HTC America Inc. (“proposed respondent”). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between HTC America Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed 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. Proposed respondent neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in this order. Only for purposes of this action, proposed respondent admits the facts necessary to establish jurisdiction.

3. Proposed respondent waives:

   A. any further procedural steps;

   B. the requirement that the Commission’s decision contain a statement of findings of fact and conclusions of law; and

   C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter

may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.

6. Proposed respondent has read the draft complaint and consent order. Proposed respondent understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. "Covered device" shall mean any desktop computer, laptop computer, tablet, handheld or mobile device, telephone, or other electronic product or device developed by respondent or any corporation, subsidiary, division, or affiliate owned or controlled by respondent that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.

2. "Covered information" shall mean individually-identifiable information from or about an individual consumer collected by respondent through a covered device or input into, stored on, captured with, or transmitted through a covered device, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e)

a Social Security number; (f) a driver's license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; (j) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; (k) an authentication credential, such as a username and password; or (l) any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, emails, text messages, photos, videos, and audio recordings.

3. "Covered device functionality" shall mean any capability of a covered device to capture, access, or transmit covered information.

4. Unless otherwise specified, "respondent" shall mean HTC America Inc. and its successors and assigns.

5. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent or its products or services, including any covered devices, use, maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of any covered information from or about consumers.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed 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. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information, including:

A. the designation of an employee or employees to coordinate and be accountable for the security program;

B. the identification of 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 assessment of the sufficiency of any safeguards in place to control these risks;

C. the identification of 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 respondent's possession or is input into, stored on, captured with, accessed or transmitted through a covered device, and assessment of the sufficiency of any safeguards in place to control these risks;

D. at a minimum, the risk assessments required by subparts B and C should include consideration of 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;

E. the design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including through reasonable and appropriate software security testing techniques, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

F. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards; and

G. the evaluation and adjustment of the security program in light of the results of the testing and monitoring required by subpart E, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

Provided, however, that this Part does not obligate respondent 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.

III.

IT IS FURTHER ORDERED that respondent shall develop security patches to fix the security vulnerabilities described in Attachment A for each affected covered device having an operating system version released on or after December 2010. Within thirty (30) days of service of this order, respondent shall release the applicable security patch(es) either directly to affected covered devices or to the applicable network operator for deployment of the security patch(es) to the affected covered devices. Respondent shall provide users of the affected covered devices with clear and prominent notice regarding the availability of the applicable security patch(es) and instructions for installing the applicable security patch(es).

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience in secure mobile programming; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and secure mobile programming; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered device functionality or covered information;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. certify that respondent’s 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 and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of HTC America Inc.*, FTC File No. 1223049. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years after the date of preparation of each Assessment required under Part IV of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts II and III of this order, for the compliance period covered by such Assessment;

B. unless covered by V.A, for a period of three (3) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:

1. all advertisements and promotional materials containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation; and

2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of HTC America Inc.*, FTC File No. 1223049. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

IX.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this ________ day of __________, 2012.

HTC AMERICA Inc.

Dated: _____

By: ______________________________________
MIKE WOODWARD, President
HTC America Inc.

Dated: _____

By: ______________________________________
SUSAN LU LYON, Esq.
Cooley LLP
719 Second Avenue, Suite 900
Seattle, WA 98104-1732
Attorney for Respondent

FEDERAL TRADE COMMISSION

Dated: _____

By:______________________________________
NITHAN SANNAPPA
JONATHAN ZIMMERMAN
Counsel for the Federal Trade Commission

APPROVED:

____
MARK EICHORN
Assistant Director
Division of Privacy and Identity Protection

____
MANEESHA MITHAL
Associate Director
Division of Privacy and Identity Protection

____
CHARLES HARWOOD
Acting Director
Bureau of Consumer Protection

ATTACHMENT A

PERMISSION RE-DELEGATION

1. Permission re-delegation occurs when one application that has permission to access covered information or covered device functionality provides another application that has not been given the same level of permission with access to that information or functionality. Because HTC failed in numerous instances to include "permission check" code in its custom, pre-installed applications on its Android-based devices, any third-party application exploiting these vulnerabilities could command those HTC applications to access various covered information and covered 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.

APPLICATION INSTALLATION VULNERABILITY

2. HTC pre-installed a custom application on its Android-based devices that could download and install applications outside of the normal Android installation process. 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.

INSECURE COMMUNICATIONS MECHANISMS

3. HTC failed to use readily-available and documented secure communications mechanisms in implementing logging applications on its devices, placing covered information at risk. Communications with logging applications should be secure to ensure that only designated applications can access the information. HTC implemented insecure communication mechanisms, as described below.

    a. HTC Loggers. HTC installed its customer support and trouble-shooting tool HTC Loggers on 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 network operators. Because HTC used an insecure communications mechanism, however, any third-party application on the user's device that could connect to the internet could exploit this vulnerability to communicate with HTC Loggers without authorization and command it to collect and transmit covered information from the device logs.

b. Carrier IQ. HTC embedded Carrier IQ diagnostics software on Android-based mobile devices and Windows Mobile-based mobile devices at the direction of network operators who used Carrier IQ to collect a variety of covered information 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. Because HTC used an insecure communications mechanism, any third-party application on the user’s device that could connect to the internet could exploit this vulnerability to communicate with the CIQ Interface, allowing it to:

   i. Intercept the covered information being collected by the Carrier IQ software; 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.

DEBUG CODE

4. During the development of its CIQ Interface for its Android-based devices, HTC activated “debug code” in order to help test whether the CIQ Interface was functioning as intended, but then failed to deactivate the code before its devices shipped for sale to consumers. As a result of the active debug code, covered information was written to the Android system log, and was accessible to any third-party application with permission to read the system log, and in many instances, was also sent to HTC.