STRANGE & CARPENTER
Brian R. Strange (Cal. Bar. No. 103252)
LACounsel@earthlink.net
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Telephone: (310) 207-5055
Facsimile: (310) 826-3210

LAW OFFICE OF JOSEPH MALLEY
Joseph H. Malley (not admitted)
malleylaw@gmail.com
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

Attorneys for Plaintiff and others similarly situated

E-FILING

ADR

FILED
MAR 22 2012
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

PSG

JAMES DOUGLAS WHITE; an individual, on behalf of himself and others similarly situated,

Plaintiff,

v.

CARRIER IQ, INC., a Delaware Corporation; HUAWEI TECHNOLOGIES CO., LTD., a Chinese Company; and HUAWEI TECHNOLOGIES USA, INC., a Texas Corporation,

Defendants.

CASE No. CV 12-01449

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §2510;
2. STORED COMMUNICATIONS ACT, 18 U.S.C. §2701;
3. CONSUMER LEGAL REMEDIES ACT, ("CLRA") CALIFORNIA CIVIL CODE § 1750;
4. UNFAIR COMPETITION LAW, CALIFORNIA BUSINESS AND PROFESSIONS CODE §17200;
5. CALIFORNIA'S COMPUTER CRIME LAW, PENAL CODE §502;
6. CALIFORNIA INVASION OF PRIVACY ACT, PENAL CODE §630;
7. SONG-BEVERLY WARRANTY ACT, CALIFORNIA CIVIL CODE § 1792
8. TEXAS DECEPTIVE TRADE PRACTICES ACT, TEXAS

By Fax

BUSINESS AND COMMERCE CODE § 17.41
9. BREACH OF EXPRESS WARRANTY
10. BREACH OF IMPLIED WARRANTY
11. NEGLIGENCE
12. TRESPASS TO PERSONAL PROPERTY/ CHATTELS
13. CONVERSION
14. UNJUST ENRICHMENT

1. Plaintiff James Douglas White ("Plaintiff"), by and through his attorneys Strange & Carpenter, and Law Office of Joseph H. Malley, P.C., brings this action on behalf of himself and all others similarly situated, against Carrier IQ, Inc. ("Carrier IQ"), Huawei Technologies Co., Ltd. ("Huawei") and Huawei Technologies USA, Inc., (collectively with Carrier IQ, "Defendants"). Plaintiff's allegations as to himself and his own actions, as set forth herein, are based upon his information and belief and personal knowledge. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §1332(d) as set forth below.

I. NATURE OF THE ACTION

2. Plaintiff brings this consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of himself and a proposed class of similarly situated consumers ("Class Members") who purchased a Huawei mobile device on which Carrier IQ's software, "IQ Agent," was installed, without notice or consent of Plaintiff. This IQ Agent software was designed by Carrier IQ and customized or authorized for customization by Huawei in order to log and collect confidential, unencrypted user data including but not limited to (1) the contents of incoming text messages; (2) the URLs of websites visited by the user; and (3) the user's GPS coordinates; among other private and personally-identifying data. IQ Agent records this confidential data on a user's mobile device in an unencrypted format so that any device software or applications with log file permission can access and review it. Carrier IQ and Huawei also have access to this confidential data and can transmit the data from a user's mobile device to remote servers at any time via hidden "text requests" sent to a user's mobile device by Carrier IQ, Huawei or other authorized third parties.

IQ Agent logs the hidden text requests and the confidential data silently so that a user has no idea that data is being collected and transmitted. IQ Agent is preinstalled or automatically updated on Huawei's mobile devices so that data logging begins the moment a user purchases or turns on the device, without notice to or consent from the user. Because the software is preinstalled or authorized for such software update by Huawei and runs as part of the device operating system, data is automatically collected and can be transmitted via wireless internet or other means, even if the device user has no carrier contract and the mobile device is not connected to a mobile network. Finally, IQ Agent runs continuously and depletes resources on the mobile device without notice to or authorization of the user, even when the mobile device is not being used. The resources depleted by IQ Agent without notice or authorization include (1) battery power; (2) device memory; (3) CPU; (4) bandwidth; and (5) text messages. A user cannot stop the IQ Agent software from running under any circumstances, and a user is unable to remove IQ Agent from the device without voiding the manufacturer's warranty.

3. Because of Defendants' actions, Plaintiff and Class Members are victims of unfair, deceptive, and unlawful business practices; wherein their privacy, financial interests, and security rights, were violated by Carrier IQ and Huawei. Plaintiff and Class Members were financially harmed by the Defendants when they purchased the Huawei mobile devices with IQ Agent, and Plaintiff would not have purchased that devices if he had known that Defendants' software could access, collect, transmit, analyze, store, and provide his confidential unencrypted data to any device software or applications with log file permission without Plaintiff's knowledge or permission. Plaintiff and Class Members were also harmed by Huawei and Carrier IQ's unauthorized use of their mobile device battery power, device memory, CPU, bandwidth and text messages.

4. Huawei manufactured and sold to Plaintiff and Class Members without notice, a defective product that included IQ Agent, specially customized by Huawei or authorized for customization by Huawei for use on its mobile device. Huawei acted individually, and in concert, with Carrier IQ to gain unauthorized access to, log, collect, and transmit Plaintiff's and Class Members' confidential, unencrypted data and to provide third-party access to this

data. IQ Agent is a native Huawei application that was installed on Huawei mobile devices with the knowledge of Huawei.

5. Carrier IQ acted independently, and in concert with Huawei, knowingly authorizing, directing, ratifying, acquiescing in, or participating in the conduct alleged herein.

6. Carrier IQ individually, and in concert with Huawei has been systematically engaged in and facilitated a covert operation of logging and tracking Plaintiff's and Class Members' confidential, unencrypted user data and utilizing Plaintiff's and Class Members' mobile device resources, violating one or more of the following:

(a) ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §2510;

(b) STORED COMMUNICATIONS ACT, 18 U.S.C. §2701;

(c) CONSUMER LEGAL REMEDIES ACT, ("CLRA") CALIFORNIA CIVIL CODE § 1750;

(d) UNFAIR COMPETITION LAW, CALIFORNIA BUSINESS AND PROFESSIONS CODE §17200;

(e) CALIFORNIA'S COMPUTER CRIME LAW, PENAL CODE §502;

(f) CALIFORNIA INVASION OF PRIVACY ACT, PENAL CODE §630;

(g) SONG-BEVERLY WARRANTY ACT, CALIFORNIA CIVIL CODE § 1792

(h) TEXAS DECEPTIVE TRADE PRACTICES ACT, TEXAS BUSINESS AND COMMERCE CODE § 17.41

(i) BREACH OF EXPRESS WARRANTY

(j) BREACH OF IMPLIED WARRANTY

(k) NEGLIGENCE

(l) TRESPASS TO PERSONAL PROPERTY/ CHATTELS

(m) CONVERSION

(n) UNJUST ENRICHMENT

///

///

II. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one class member is of diverse citizenship from Defendants; there are more than 100 class members nationwide; and the aggregate amount in controversy exceeds $5,000,000 and minimal diversity exists.

8. Venue is proper in this District under 28 U.S.C. §1391(b) and (c) against Defendants. A substantial portion of the events, conduct and omissions giving rise to the violations of law complained of herein occurred in this District. Carrier IQ's principal executive offices and headquarters are located in this District at 1200 Villa Street, Suite 200, Mountain View, CA 94041.

9. This Court has personal jurisdiction over the Defendants because Carrier IQ maintains its corporate headquarters in, and the events, conduct and omissions giving rise to the violations of law complained herein occurred in California. Huawei conducts business in California and is engaged in the acts alleged herein in California.

10. This Court also has subject matter jurisdiction over all causes of action and the Defendants implicated therein pursuant to 28 U.S.C. §1332(d), and because this action arises in part under a federal statute and this Court has jurisdiction pursuant to 18 U.S.C. §2710(c) which confers jurisdiction in the United States District Court for actions related to the Electronic Communications Privacy Act 18 U.S.C. §2510 and the Stored Communications Act, 18 U.S.C. §2701.

11. **INTRADISTRICT ASSIGNMENT**: Pursuant to Civil Local Rule 3-2(e), this case shall be assigned to the San Jose Division as it arises from Santa Clara County where Carrier IQ is headquartered and where the actions alleged as the basis of this claim took place.

III. PARTIES

12. Plaintiff James Douglas White ("White") is a citizen and resident of Seabrook, Texas (Harris County). On information and belief, White incorporates all allegations within this complaint. White is a representative of the class ("Class"), as defined within the Class Allegations. In or around November 2011, White purchased a Huawei Ascend II mobile device

that was preinstalled or automatically updated with IQ Agent, and used such mobile device on one or more occasions during the class period in Texas.

13. White was not aware that IQ Agent was installed on his Huawei device, and was not aware that every time he used his Huawei device, IQ Agent was logging and collecting his confidential incoming text messages; the URLs of websites he visited; and his actual GPS coordinates; among other private and personally-identifying data. He also was not aware that IQ Agent made this confidential, unencrypted data available on White's mobile device log so that *any* device software or applications with log file permission could access it. Finally, White was not aware that IQ Agent depleted his mobile device battery power, device memory, CPU, bandwidth and text messages, even while he was not using his device. The IQ Agent software does not show up under the application launch list on White's device.

14. Carrier IQ is a Delaware corporation that maintains and has maintained at all relevant times its headquarters at 1200 Villa Street, Suite 200, Mountain View, CA, 94041 (Santa Clara County, California). Carrier IQ does business throughout the United States, and in particular, does business in the State of California and in this County.

15. Huawei Technologies Co., Ltd. is a Chinese company with its principal place of business located at Bantian, Lonnggang District, Shenzhen 518129, P.R. China. Huawei Technologies Co., Ltd. has a United States subsidiary of Huawei Technologies USA, Inc. Huawei does business throughout the United States, and in particular, does business in the State of California and in this County.

16. Huawei Technologies USA, Inc. is a Texas corporation, a subsidiary company of Huawei Technologies Co., Ltd., a China corporation, with its principal place of business located at 5700 Tennyson Pkwy Suite 500, Plano, Texas, 750247157. Huawei does business throughout the United States, and in particular, does business in the State of California and in this County.

IV. PLAINTIFF'S EXPERIENCE

17. At all relevant times herein, Plaintiff was and is a resident of Texas. During the class period, Plaintiff owned and operated one or more Huawei mobile devices installed with

IQ Agent without Plaintiff's knowledge.

18. On one or more occasions during the class period, Plaintiff accessed and used his Huawei mobile device to receive text messages and visit websites in his city of residence and elsewhere.

19. During the relevant class period, the IQ Agent software was "hidden" and did not appear on the application launch menu on Plaintiff's Huawei mobile device. During the relevant class period, Plaintiff was unaware that IQ Agent populated and logged incoming text messages, visited URLs and GPS location data on his device log files. Plaintiff was also unaware that this confidential data was available, unencrypted, to all software and programs with log file permission running on his device. Additionally, he was unaware that IQ Agent had the mechanisms to, and did, transmit user data from Plaintiff's devices to remote servers via periodic scheduling, WAP push requests, and text requests.

20. During the relevant class period, IQ Agent, customized in part by Huawei, was "hidden" and did not appear on the launch list of applications and software installed on Plaintiff's Huawei mobile device.

21. In or around February 2012, Plaintiff became aware of information related to the tracking activities of Carrier IQ and Huawei.

22. Plaintiff's mobile devices revealed that the IQ Agent software resided on his device without notice to Plaintiff or authorization from Plaintiff.

23. Plaintiff considers information about his received text messages, visited websites and GPS location to be in the nature of confidential and personal information that he protects from disclosure, including by controlling his mobile device's privacy settings for acceptance or rejection. Plaintiff was not made aware by Defendants of the existence of IQ Agent on his mobile device or the logging, collection and transmission of his mobile device data.

24. Plaintiff also considers his device battery power, device memory, CPU, bandwidth and text messages to be valuable personal property that he protects from unauthorized use by third parties, including by controlling what software and applications have

access to those resources. Plaintiff was not made aware by Defendants of the existence of IQ Agent on his mobile device or the depletion of his device battery power, device memory, CPU, bandwidth and text messages by that software.

25. It is Plaintiff's belief that the Carrier IQ software, customized or authorized for customization in part by Huawei, was logging, collecting and transmitting confidential user data on his mobile devices, thus permitting one or more objects within his mobile device to be used for tracking and analysis by Defendants and/or third parties for the purposes of monitoring and profiling his mobile device activities. Plaintiff did not receive notice of the installation of a tracking identifier, did not consent to its installation, and did not want a tracking identifier to be installed on his mobile device. Moreover, Plaintiff did not authorize Defendants to log, collect, transmit, or store his confidential mobile device data without notice or express consent. Such software was running on Plaintiff's mobile device and collecting and transmitting Plaintiff's data without notice or authorization, utilizing Plaintiff's battery power, device memory, CPU, bandwidth and limited text messages without notice or authorization, even when Plaintiff stopped actively using the device.

26. In selecting the Huawei mobile device over the service and goods of other competing mobile device manufacturers, Plaintiff reasonably expected that his confidential user data would not be accessed, logged and transmitted to third parties without his knowledge and consent. He also reasonably expected that his mobile device resources would not be depleted without his knowledge or control.

27. Had Plaintiff known that the Huawei device he purchased would include software that provided third party access to his confidential user data and his mobile device resources without notice to or authorization by Plaintiff, Plaintiff would have not purchased that device.

28. Plaintiff was harmed by Defendants' practices, including but not limited to the following:

(a) Costs to purchase the defective Huawei mobile device;

(b) Violations of Plaintiff's legally protected federal, state and common

law rights of privacy, especially related to unencrypted logging, storage and transmission of Plaintiff's confidential user data;

(c) Time and expense to remedy the effects of Defendants' actions;

(d) Time and expense to repair Plaintiff's mobile devices and remedy the impaired operability caused by the Defendants;

(e) Loss of property due to the inability to re-sell Plaintiff's and Class Members' mobile devices due to the Carrier IQ application; and

(f) Financial harm by the Defendants' unauthorized use of Plaintiff's mobile device resources during the unauthorized process of logging and transmitting user data.

29. It is Plaintiff's belief that IQ Agent's logging, collection and transmission of confidential user data on his mobile device permitted one or more objects within his mobile devices to be used for tracking and analysis by Defendants and/or third parties, thus his mobile device data was obtained in an effort to monitor and profile his mobile device activities. Plaintiff did not receive notice of the installation of a tracking identifier, did not consent to its installation, and did not want a tracking identifier to be installed on his mobile device. Moreover, Plaintiff did not authorize Defendants to log, collect, transmit, or store his confidential mobile device data without notice or express consent.

30. Defendants' business practices unfairly wrested from Plaintiff control over his user data privacy and control over his device resources. Defendants' logging, collection and unencrypted disclosure of Plaintiff's confidential user data violates user expectations, diminishes user privacy, and contradicts the Manufacturer's Warranty. Defendants caused harm and damages to Plaintiff's finite device resources, thus preventing Plaintiff from using the device for his intended purposes and resulting in instability issues.

V. COMMON EXPERIENCES BETWEEN PLAINTIFF AND CLASS MEMBERS

31. At all relevant times herein, the sequence of events, and consequences common to Plaintiff and Class Members, made the basis of this action, include, but are not limited to the following:

(a) Plaintiff and Class Members are individuals in the United States who purchased and used a Huawei mobile device that had IQ Agent software installed and/or authorized for installation by Huawei, without notice or consent;

(b) Huawei, a mobile device manufacturer, had entered into a legally binding contract with Carrier IQ to host the IQ Agent software on its mobile device;

(c) Carrier IQ was aware that Huawei had preinstalled IQ Agent on Plaintiff's and Class Members' mobile devices. It was also aware that Huawei had customized IQ Agent, and that IQ Agent was "hidden" and did not appear in the launch list of applications installed on Plaintiff's and Class Members' mobile devices;

(d) Plaintiff and Class Members accessed and used their Huawei mobile devices that had the preinstalled or uploaded IQ Agent software application;

(e) Carrier IQ collected confidential user data from Plaintiff's and Class Members' mobile devices without consent of, or notice to, Plaintiff and Class Members;

(f) Carrier IQ sent Plaintiff's and Class Members' unencrypted confidential mobile device data to its servers located in California without notice to or authorization from Plaintiff and Class Members;

(g) Huawei transmitted, and/or allowed access to Plaintiff's and Class Members' confidential mobile device data, without notice or authorization, to Huawei and *any* software with log file access on Plaintiff's and Class Members' devices. Upon information and belief, this confidential data was unencrypted when stored in the log file and during at least some part of its transmission;

(h) Carrier IQ created a database related to Plaintiff's and Class Members' mobile device data and activities, to assist the Defendant's tracking scheme. Such tracking could not be detected, managed or deleted, and provided, in whole or part, the collective mechanism to track Plaintiff and Class Members, without notice or consent;

(i) Carrier IQ conducted systematic and continuous surveillance of the Plaintiff's and Class Members' mobile device activity from its headquarters in California which continues to date;

(j) Carrier IQ copied, used, and stored Plaintiff's and Class Members' mobile device data in California after it knowingly accessed, without authorization, Plaintiff's and Class Members' mobile devices;

(k) Carrier IQ obtained and retained the data in California for a period that far exceeded the purpose claimed by Carrier IQ for obtaining the data;

(l) Carrier IQ obtained individually, and in concert with Huawei, Plaintiff's and Class Members' confidential user data, derived, in whole or part, from its monitoring the mobile device activities of Plaintiff and Class Members. This sensitive information includes, but is not limited to, incoming text messages, visited URLs and GPS coordinates;

(m) Huawei and Carrier IQ failed to notify and warn Plaintiff and Class Members of Carrier IQ's logging and tracking activities involving their mobile devices before, during, or after the unauthorized practices so that Plaintiff and Class Members were unable to take appropriate actions to opt-out of the unauthorized surveillance by Defendants and other third parties;

(n) Huawei failed to block access to, and void the licensing agreements of Carrier IQ after it received notice of Carrier IQ's tracking actions made the basis of this action;

(o) Carrier IQ and Huawei failed to provide any terms of service or privacy policy related to the use of IQ Agent for tracking Plaintiff's and Class Members' mobile activities, or provide an updated privacy policy or any notice alerting users of its activity, made the basis of this action so that Plaintiff and Class Members had no notice of such activities, nor the ability to mitigate their harm and damage after the fact;

(p) Defendants converted Plaintiff's and Class Members' mobile device data, including but not limited to their incoming text messages, visited URLs and GPS coordinates; and

(q) Defendants depleted Plaintiff's and Class Members' mobile device resources while running the IQ Agent software, including the device battery power, device

memory, CPU, bandwidth and text messages.

32. Plaintiff and Class Members involved with the Defendants were harmed by Defendants' practices, including but not limited to the following:

(a) Violations of Plaintiff's and Class Members' legally protected federal, state and common law rights of commerce and privacy, especially related to unencrypted transmission of Plaintiff and Class Members' confidential and sensitive user data;

(b) Financial harm due to the costs to purchase the defective Huawei mobile device;

(c) Financial harm due to the time and expense to remedy the effects of Defendants' actions;

(d) Financial harm due to the time and expense to repair Plaintiff's and Class Members' mobile devices and remedy the impaired operability caused by the Defendants;

(e) Financial harm due to the loss of property due to the inability to re-sell Plaintiff's and Class Members' mobile devices due to the Carrier IQ application;

(f) Financial harm due to the loss of property due to the unauthorized access and use of Plaintiff's and Class Members' confidential user data, depriving Plaintiff and Class Members of such possession and use;

(g) Financial harm due to the Defendants' unauthorized use of Plaintiff's and Class Member's mobile device's battery power, device memory, CPU, bandwidth and text messages during the unauthorized process of obtaining user data;

VI. FACTUAL ALLEGATIONS

A. Background

33. On October 26, 1999 the Wireless Communication and Public Act of 1999 was enacted and became known as the "e911 Act." It was an amendment to the Telecommunication Act of 1996. The purpose of the bill was to promote and enhance public safety through the use of 911 as universal assistance number. The Federal Law mandated that mobile phones be embedded with a Global Positioning System ("GPS") chip, which could calculate a user's

coordinates to within a few yards by receiving signals from satellites. This law enacted to aid those in harm's way, resulted in the computing industry developing hardware and software to assist in the development of this technology or mobile devices provided Carrier IQ the impetus to originate a business plan to take advantage of the benefit of embedded GPS chips in all mobile phones for its own commercial benefit:

> This confluence of circumstances and events— rapid adoption of new wireless technologies, improved resiliency of service, increased data transmission rates, the e911 law requiring homing chips, and market precedents which show that mobile device users are willing to pay for wireless services or applications— establish the feature-rich wireless station as an increasingly logical and compelling channel for the free flow of communications, information, entertainment and commerce.

United States Patent No.: US 7,609,650 B2, COLLECTION OF DATA AT TARGET WIRELESS DEVICES USING DATA COLLECTION PROFILES, Assignee: Carrier IQ, Inc., Mountain View, CA (US), Filed: July 5, 2005.

34. Carrier IQ's software is reportedly installed in excess of one hundred and fifty million (150,000,000) mobile devices, including mobile devices manufactured by Huawei. These devices installed with IQ Agent are inherently defective, and Defendants falsely advertised, marketed and distributing these mobile devices, without disclosure of the material facts about the defect, misrepresenting the performance of the devices, violating express and implied warranties, thus rendering the mobile devices unable to be used for their intended purposes. Such activities resulted in a pattern of covert mobile device surveillance, wherein Defendants installed IQ Agent on Plaintiff's and Class Members' mobile device without authorization and consent, thereby committing unauthorized access, collection, storage, and use of, the mobile device and data derived from the Plaintiff's and Class Members' use of the mobile devices and transmitting information, code, and commands to collect, monitor, and remotely store non-anonymized Plaintiff's and Class Members' confidential mobile device data. Defendants' unauthorized access of this confidential, unencrypted data also allowed access to *all* software and applications with log file access so that Plaintiff's and Class Members' data could be transmitted by multiple unknown parties at any time, *like a pac-man*

creeping 150 million mobile phones and "calling home."

35. The Huawei-version of the software IQ Agent, is currently preinstalled or authorized for remote update installation by Huawei on its Carrier IQ-enabled mobile devices and was also installed via software updates on older Huawei devices.

B. Carrier IQ: " See What Content They Consume Even Offline"

36. According to Carrier IQ, the software is designed to monitor, manage and support mobile devices deployed across mobile operators, service providers and enterprises. Carrier IQ's website explains:

> [IQ Agent] provides a level of visibility into true customer experience that was, previously unavailable in the mobile industry. [IQ Agent] uses data directly from the mobile phone itself to give a precise view of how users interact with both their phones and the services delivered through them, even if the phone is not communicating with the network.

http://www.carrieriq.com/overview/IQInsightExperienceManager/index.htm (last visited December 5, 2011).

37. IQ Agent is a monitoring software that runs continuously in the background reportedly to monitor device and application performance. When a particular event or error associated with the device occurs, the software collects data associated with the event or error and may upload it either in real time or at a later time to its data repository for analysis.

38. During the use of a mobile device in a mobile communication network, parameter data defining conductors associated with the mobile device and operation is generated. The mobile device also generates event data defining events of the mobile device for the associated mobile user. Such events are referred to as "Trigger points."

39. IQ Agent is programmed to obtain qualifying characteristics which may include device type, such as manufacturer and model, available memory and battery life, the type of applications resident on the device, the geographical location of the device, usage statistics, including a "profile" that characterizes a user's interaction with a device, and the profile. Such mobile device characteristics are referred to as "metrics."

40. Carrier IQ's patent for "data collection associated with components and services

of a wireless communication network" explains the breadth of this data collection,

> Carrier IQ is able to query any metric from a device. A metric can be a dropped call because of lack of service. The scope of the word metric is very broad though, including device type, such as manufacturer and model, available memory and battery life, the type of applications resident on the device, the geographical location of the device, the end user's pressing of keys on the device, usage history of the device, including those that characterize a user's interaction with a device.

http://www.faqs.org/patents/app/20110106942 (last accessed December 2, 2011).

41. Carrier IQ provides a platform for data collection and management system to dynamically generate and download to a population of wireless devices rule-based data collection by coding its software to function when interfaced with "trigger points" and to obtain "metrics." Data collection profiles may be generated manually by a network administrator, a software developer or other personnel involved in the operation of the network or "network administrators," created offline as a portion of a data analysis solution, or automatically generated based on network.

42. This parameter data and event data may be used to monitor a network or used by an advertising system of the mobile communications network to select an advertisement and the timing of the display of the advertisement, and is necessary due to the problems associated with mobile advertising.

43. Mobile Internet advertising currently consists of streaming graphic files, in real time, into content rendered by a user's mobile device browser. Mobile advertising systems though lack reliable browser tracking while traditional online advertising relies on the use of browser cookies. Implementations inherent in conventional mobile ad serving have effectively prevented mobile advertising from being effective because of its inability to obtain mobile device "uniqueness." In order to obtain such uniqueness, the mobile advertising industry sought a means to obtain unique device identifiers which provide a unique reference to individual mobile devices. Unlike traditional cookies, such identifiers are hard coded into a user's phones software, and thus a user has no ability to disable mobile device identifiers.

44. Mobile Device "tracking" by use of mobile device identifiers is not exactly

comparable to any other type of tracking by advertising networks. This is not anonymous data – but an exact ID that's unique to each physical device, and if merged, with mobile device activities, including but not limited to, identifying phone accessed user's physical locations, time of transmission, applications downloaded, social network IDs, providing unlimited advertising opportunities (i.e., commercial value). Recording of a user's GPS, without their knowledge or consent also creates a security harm to the mobile device user. When tracking a user's location data on the mobile device, it is calculated to eight decimal points that can be far more exact and accurate than any sort of geographically-based IP address look-up on the web. Instead of getting a general location, location data on a GPS-enabled mobile can identify user's precise latitude and longitude.

45. The mobile device industry thus sought the technical means of synchronizing tracking code so that information about individual consumer behavior on mobile devices could be shared between companies and the unique device identifiers used in the majority of mobile devices would be put to this purpose. Carrier IQ initial patent was able to extract unique Identifiers from mobile devices:

Patent Title: COLLECTION OF DATA AT TARGET WIRELESS DEVICES USING DATA COLLECTION PROFILES SYSTEMS AND METHODS FOR USING DISTRIBUTED NETWORK ELEMENTS TO IMPLEMENT MONITORING AND DATA COLLECTION CONCERNING SELECTED NETWORK PARAMETERS.

Patent No.: US 7,609,650 B2

Assignee: Carrier IQ, Inc., Mountain View, CA (US)

Filed: July 5, 2005

Inventor: Konstantin Othmer

46. The dilemma facing the mobile advertising industry is that once the mobile device data was extracted, a system and method was needed for wireless devices to use data for mobile advertising. While Carrier IQ may have concentrated on extraction of mobile device metrics, other companies were interested in assisting the mobile advertising networks to use mobile device data.

C. IQ Agent Technology

i. *IQ Agent Collection of Unencrypted User Data Via Device "Log File"*

47. To monitor use of a mobile device, IQ Agent collects user data by utilizing the mobile device's "log file"—a storage file that records certain actions or events that occur on the device in real time, such as when the device is turned on or disconnected from a power source. The log file can be examined by any software or application with Android operating system permission to view it. Data is populated on the log file when software such as Huawei IQ Agent prompts the operating system to append an entry into the log file.

48. IQ Agent specifically prompts mobile operating systems to populate log file data for a number of confidential events, including the following:

(a) the contents of all incoming text messages;

(b) the URLs of all websites visited; and

(c) a user's GPS coordinates.

IQ Agent records this data on the log file in an unencrypted format, so the data is available to *any* device software or applications with log file permission. In other words, *any* software or application with Android operating system access can transmit and collect the user's incoming text messages, visited URLs and/or GPS coordinates because of the log file entries populated by IQ Agent. This log file access is typically granted to software and applications that a user installs from the market and a user would have no reason to believe that in granting "log file" access, he or she is also granting access to this unencrypted, confidential data.

49. This puts users' confidential data at great risk. Even if the authors of the software and applications running on the mobile device have the best intentions, if these authors incorporate any third party code into their own software or applications (which is quite common), the users' data is exposed to these other third parties and is jeopardized.

ii. *IQ Agent Transmission of User Data Via Periodic Scheduling and Remote Triggering*

50. IQ Agent provides two mechanisms to transmit confidential data off the device:

periodic scheduling and remote triggering. The IQ Agent software provides specific "collection points" where the confidential data will be sent. One of these "collection points" encoded in the software is http://collector.sky.carrieriq.com:7001/collector/c?cm_sl=5. Data transmitted to this Carrier IQ server will remain unencrypted and unprotected during data transmission and receipt.

51. IQ Agent can prompt a user's mobile device to send confidential data to Carrier IQ's server on a periodic schedule, e.g., once a week or once a month. It can also prompt a user's device to send confidential data at any time via a "WAP push request" or a "text request." A WAP push request is a specially-formatted message delivered to the device over a mobile data or internet connection requesting transmission of data from the device. A user would be unaware that a WAP push request had been made to their device. A text request is a standard text message sent to the device with contents beginning with "//CM" or "//IQ." The contents of that message direct the device to transmit data from the device. This text message is "suppressed" or hidden to the operator, meaning that the user does not see the text message and is unaware that Carrier IQ or some other party has requested transmission of confidential data from the device.

iii. *IQ Agent Continuous Unauthorized Data Logging and Transmission*

52. IQ Agent begins logging confidential user data the moment the user first purchases the mobile device and turns it on, without notice to or consent from the user. IQ Agent logs this data silently so that users have no knowledge the data is being logged or is available to any device software or applications with log file permission. The data is also transmitted silently so users are unaware that confidential data is being broadcast from their devices. Data is logged and transmitted even when the device is not in use.

53. An average user will have no knowledge that the IQ Agent software is even running on his or her device, and the IQ Agent software does not appear on the device's application launch menu.

54. A user is unable to stop the Carrier IQ software from running. When a user manually turns off the IQ Agent software, it automatically restarts itself seconds later. A user is

unable to delete or remove the IQ Agent software from the device without voiding Huawei's manufacturer's warranty.

55. Because the software is preinstalled or authorized for automatic remote installation by Huawei and runs as part of the device operating system, data is continuously collected and can be transmitted via wireless internet or other means, even if the device user has no carrier contract and the mobile device is not connected to a mobile network.

iv. *IQ Agent Depletion of Resources*

56. Because IQ Agent runs continuously and silently, it depletes device resources without notice to or authorization from the user. These depleted resources include:

(a) battery power (required to run the device while activity such as data logging and transmission occurs);

(b) device memory (used to log confidential user data and receive and respond to WAP push requests and/or text requests);

(c) CPU (also known as "central processing unit" used to process the instructions and perform the functions required by the IQ Agent software);

(d) bandwidth (used to transmit and receive data according to IQ Agent instructions); and

(e) text messages (IQ Agent's hidden text request function indicates a text has been received by the user even when the user cannot see it, and may result in a charges to users who pay for a finite number of texts per month).

D. Huawei's Warranty

57. There is no choice to "opt in" to Carrier IQ's data collection and transmission by downloading IQ Agent since in many cases it is preinstalled or installed via remote automatic update on Plaintiff's and Class Members' mobile devices. Users cannot uninstall it, block it, or cease its actions. Huawei and Carrier IQ provide Plaintiff and Class Members no notice of this software or the functions it performs.

58. Huawei's Manufacturer's Warranty for the Huawei mobile devices does not mention or disclose the existence of the IQ Agent software on the device or the functions that

software performs.

59. Huawei's Manufacturer's Warranty states that the Warranty will be void if a user alters or impairs the operating system, which would include deleting or attempting to delete the IQ Agent software from the device.

E. Defendants' Harmful Business Practices

60. Defendants' business practice unfairly wrests the user's control and consumes the resources of the Plaintiff's and Class Members' mobile devices by gathering information, populating such information in an unencrypted format in their mobile log file, and transferring such information to storage for subsequent use. Defendants caused harm and damages to Plaintiff's and Class Members' mobile devices' finite resources, depleted and exhausted its battery power, memory, CPU bandwidth and text, thus causing an actual inability to use it for its intended purposes and resulting in instability issues.

61. Defendants' collection and disclosure of this personal information violates user expectations, diminishes user's privacy, and contradicts Huawei's own representations. These business practices are unfair and deceptive trade practices as set forth further below.

62. Defendants' activities, made the basis of this action include, but are not limited to, economic harm due to the unauthorized use of Plaintiff's and Class Members' bandwidth, the amount of data that can be transmitted across a channel in a set amount of time. Any transmission of information on the internet includes bandwidth. Similar to utility companies, such as power or water, the "pipeline" is a substantial capital expenditure, and bandwidth usage controls the pricing model. Hosting providers charge user's for bandwidth because their upstream provider charges them and so forth until it reaches the "back bone providers". Retail providers purchase it from wholesalers to sell its consumers.

63. Defendants' activities made the basis of this action consume vast amounts of bandwidth, slowing a user's internet connection by using their bandwidth, in addition to diminishing the mobile devices "battery life," CPU and device memory in order to send, store and retrieve metric data.

64. Plaintiff and Class Members were afforded only a millisecond of time after

(a) whether Defendants omitted, misrepresented or otherwise failed to notify Class Members of the fact that IQ Agent was installed on Plaintiff's and Class Members' mobile devices;

(b) whether Defendants omitted, misrepresented or otherwise failed to notify Class Members of the fact that IQ Agent logs unencrypted data in the device log file that includes incoming text messages, visited URLs and GPS location coordinates;

(c) whether Defendants omitted, misrepresented or otherwise failed to notify Class Members of the fact that IQ Agent utilizes finite device resources such as battery power, device memory, CPU, bandwidth and text messages;

(d) whether Defendants' conduct violates the federal Electronic Communications Privacy Act

(e) whether Defendants' conduct violates the federal Stored Communications Act;

(f) whether Defendants' conduct violates California's Consumers Legal Remedies Act;

(g) whether Defendants' conduct violates Texas's Deceptive Trade Practices Act;

(h) whether Defendants were negligent in their failure to disclose the presence of IQ Agent on Plaintiff's and Class Members' mobile devices and/or their failure to seek Plaintiff's and Class Members' consent prior to logging, collecting and transmitting confidential user data;

(i) whether Defendants' conduct constitutes trespass; and

(j) whether Defendants were unjustly enriched from their conduct, and whether they must disgorge profits to Plaintiff and Class Members.

71. Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff has no interests antagonistic to those of the Class and is subject to no unique defenses.

72. Plaintiff will fairly and adequately protect the interests of the Class and has retained attorneys experienced in class and complex litigation.

activating their Huawei mobile device before IQ Agent intentionally, and without users' authorization and consent, accessed Plaintiff's and Class Members' mobile device. While only the most tech savvy mobile device users are familiar with IQ Agent's activity, even a more finite amount of individuals know how to actually remove IQ Agent, let alone recognize the risk of that software to their confidential user data.

VII. CLASS ACTION ALLEGATIONS

65. Plaintiff brings this action pursuant to Rule 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure on behalf of themselves and all others similarly situated, as members of the proposed nationwide Class ("Nationwide Class"), defined as follows:

> All consumers in the United States who purchased and used a Huawei mobile device on which the IQ Agent software resides from March 11, 2007 to the date of Class certification.

66. Plaintiff also bring certain of the claims on behalf of itself and a portion of the class described as the Texas subclass ("Texas Subclass"), defined as follows:

> All consumers residing within the State of Texas who purchased and used a Huawei mobile device on which the IQ Agent software resides from March 11, 2007 to the date of Class certification.

67. Excluded from the Nationwide Class and Texas Subclass are the officers, directors, and employees of Carrier IQ and Huawei, and their respective legal representatives, heirs, successors and assigns.

68. This action is brought as a class action and may properly be so maintained pursuant to the provisions of Federal Rule of Civil Procedure 23. Plaintiff reserves the right to modify the Nationwide Class and the Texas Subclass definitions and the class period pursuant to discovery that is conducted hereafter.

69. The members of the Class are so numerous that joinder of all members would be impracticable. Plaintiff estimates that there are hundreds of thousands of consumers who purchased Huawei mobile devices installed with the IQ Agent software.

70. There are questions of law and fact common to the members of the Class that predominate over any questions affecting only individual members, including:

73. A class action is superior to other available methods for the fair and efficient adjudication of this controversy for the following reasons:

(a) It is economically impractical for each member of the Class to prosecute individual actions;

(b) The Class is readily definable;

(c) Prosecution as a class action will eliminate the possibility of repetitious litigation;

(d) A class action will enable claims to be handled in an orderly and expeditious manner;

(e) A class action will save time and expense and will ensure uniformity of decisions; and

(f) Plaintiff does not anticipate any difficulty in the management of this litigation as a class action.

74. Defendants have acted and refused to act on grounds that apply generally to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

75. Plaintiff believes that notice to the Class is necessary and proposes that notice of this class action be provided by individual mailings to Class members and/or by publication in national publications.

VIII. CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the Electronic Communications Privacy Act 18 U.S.C. § 2510

Against All Defendants

76. Plaintiff incorporates by reference all paragraphs previously alleged herein.

77. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

78. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, referred to as "ECPA," regulates wire and electronic communications interception and

interception of oral communications, and makes it unlawful for a person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

79. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiff's and Class Members' electronic communications, without knowledge, consent, or authorization.

80. At all relevant times, Defendants engaged in business practices of intercepting and collecting the Plaintiff's and Class Members' confidential electronic communications which included incoming text messages, URLs of websites viewed and GPS coordinates from within their mobile devices. Once Defendants obtained this confidential personal information, Defendants used it to aggregate mobile device data regarding Plaintiff's and Class Members' uses of their mobile devices. Defendants also made this confidential and unencrypted data available to any device software or application with log file access, further violating Plaintiff's and Class Members' privacy.

81. The contents of data transmissions from and to Plaintiff's and Class Members' personal computers constitute "electronic communications" within the meaning of 18 U.S.C. §2510.

82. Plaintiff and Class Members are "person[s] whose ... electronic communication is intercepted ... or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

83. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept Plaintiff's and Class Members' electronic communications.

84. Defendants violated 18 U.S.C. § 2511(1)(c) by intentionally disclosing, or endeavoring to disclose, to any other person the contents of Plaintiff's and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiff's and Class Member's electronic communications.

85. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiff's and Class Members' electronic communications.

86. Defendants' intentional interception of these electronic communications without Plaintiff's or Class Members' knowledge, consent, or authorization was undertaken without a facially valid court order or certification.

87. Defendants intentionally used such electronic communications, with knowledge, or having reason to know, that the electronic communications were obtained through interception, for an unlawful purpose.

88. Defendants unlawfully accessed and used, and voluntarily disclosed, the contents of the intercepted communications to enhance their profitability and revenue through manufacturer contracts and advertising. This access and disclosure was not necessary for the operation of Defendants' system or to protect Defendants' rights or property.

89. The Electronic Communications Privacy Act of 1986, 18 USC §2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the ECPA.

90. Defendants are liable directly and/or vicariously for this cause of action. Plaintiff therefore seeks remedy as provided for by 18 U.S.C. §2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and a reasonable attorney's fee and other litigation costs reasonably incurred.

91. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy. Defendants exposed Plaintiff's and Class Members' personal information to any third party software or application with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted format. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members'

mobile devices including battery power, device memory, CPUs, and bandwidth. Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden text message that was sent by Defendants.

92. Plaintiff and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the above-described violations. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's and Class Members' remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 2510.

SECOND CAUSE OF ACTION

Violation of the Stored Communications Act, 18 U.S.C. §2701

Against All Defendants

93. Plaintiff incorporates the above allegations by reference as though fully set forth herein.

94. The Stored Communications Act prohibits persons from accessing without authorization a device through which an electronic communications service is provided (18 U.S.C. §2701).

95. Defendants were engaged in the sale of mobile devices to consumers during the class period.

96. Defendants intentionally accessed and collected the personal data of Plaintiff and Class Members on their mobile devices without notice or authorization, including incoming text messages, URLs of websites viewed and GPS coordinates.

97. As a result of Defendants' unlawful violation of this section, Plaintiff and Class Members have been damaged by among other things, failing to receive the benefits of a product impliedly represented to them as secure as to their personal information. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including

violation of their rights of privacy. Defendants exposed Plaintiff's and Class Members' personal information to any third party software or application with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members' mobile devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover, Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden text message that was sent by Defendants.

98. Plaintiff and Class Members have been harmed by Defendants' unlawful violations of this section and are therefore entitled to relief in the form of damages, costs and disbursements, including costs of investigation and reasonable attorney's fees and are entitled to equitable relief as determined by this Court.

THIRD CAUSE OF ACTION

Violation of the Consumer Legal Remedies Act

("CLRA") California Civil Code § 1750, *et seq.*

Against All Defendants

99. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

100. In violation of Civil Code §1750, et seq. (the "CLRA"), Defendants have engaged and are engaging in unfair and deceptive acts and practices in the course of transactions with Plaintiff, and such transactions are intended to and have resulted in the sales of services to consumers. Plaintiff and Class Members are "consumers" as that term is used in the CLRA because they sought or acquired Defendants' goods or services for personal, family, or household purposes.

101. At all relevant times, Defendants' business practices of selling Huawei mobile devices installed or updated with IQ Agent software, were goods Plaintiff and Class Members obtained for use. Defendants' scheme to offer such goods misled Plaintiff and Class Members about the nature and integrity of the Huawei mobile devices since Defendants intended to use such for mobile device tracking, collection of confidential, unencrypted user data, and

depletion of consumer resources, including battery power, device memory, CPUs, and bandwidth. Defendants also charged consumers for every hidden text message that was sent by Defendants.

102. Defendants represented that their services had characteristics, uses, and benefits that they do not have, in violation of Civil Code § 1770(a)(5). Defendants represented privacy and "reliable, worry-free service" as a characteristic of the mobile devices that they did not have. Defendants intercepted and collected Plaintiff's and Class Members' electronic communications which included incoming text messages, URLs of websites viewed and GPS coordinates from within their mobile devices. Once Defendants obtained this personal information, Defendants used it to aggregate mobile device data of Plaintiff and Class Members as they used their mobile device. Defendants made this personal information available, unencrypted, to any third party software or applications with log file access on the device and further violated Plaintiff's and Class Members' privacy.

103. In addition, Defendants' modus operandi constitutes an unfair practice in that Defendants knew, or should have known, that consumers care about the status of personal information regarding visited websites, GPS location and text privacy but were unlikely to be aware of the manner in which Defendants failed to fulfill their commitments with respect to the consumers' privacy.

104. Defendants' acts and practices were deceptive and unfair because they were likely to mislead the members of the public to whom they were directed.

105. Plaintiff and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy. Defendants exposed Plaintiff's and Class Members' personal information to any third party software or application with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members' mobile devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover, Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden

text message that was sent by Defendants.

106. Plaintiff, on behalf of himself and on behalf of each member of the Class, shall seek individual restitution, injunctive relief, and other relief as the Court deems just and proper.

107. Pursuant to California Civil Code, Section 1782, Plaintiff will notify Defendants in writing of the particular violations of Civil Code, Section 1770 and demand that Defendants rectify the problems associated with its behavior detailed above, which acts and practices are in violation of Civil Code Section 1770.

FOURTH CAUSE OF ACTION

Violation of Unfair Competition California Business and Professions Code § 17200

Against All Defendants

108. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

109. In violation of California Business and Professions Code Section 17200 et seq., Defendants' conduct in this regard is ongoing and includes, but is not limited to, unfair, unlawful and fraudulent conduct.

110. At all relevant times, Defendants' business practices as alleged above constitute unlawful, unfair and fraudulent business acts and practices.

111. Defendants engaged in these unfair and fraudulent practices to increase their profits. Plaintiff and Class Members were injured and damaged by being forced to relinquish—without consent or knowledge—confidential and personal user data, device battery power, device memory, CPUs, and bandwidth. Plaintiff and Class Members were also unfairly charged for every hidden text message that was sent by Defendants.

112. By engaging in the above-described acts and practices, Defendants have committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiff and the Class have suffered injury-in-fact and have lost money and/or property.

A. <u>Unlawful Business Act and Practices</u>

113. Defendants' business acts and practices are unlawful, in part, because they violate the Electronic Communications Privacy Act, 18 U.S.C. Section 2510 which prohibits any person from willfully intercepting or endeavoring to intercept, or procuring any other

person to intercept or endeavor to intercept, any wire, oral, or electronic communication, including incoming text messages.

114. Defendants' business acts and practices are also unlawful in that they violate the Stored Communications Act, 18 U.S.C. Section 2701, California Consumer Legal Remedies Act, California Civil Code §1750, and California Penal Code, § 502 among other statutes.

B. Unfair Business Act and Practices

115. Defendants' business acts and practices are unfair because they cause harm and injury-in-fact to Plaintiff and Class Members and for which Defendants have no justification other than to increase revenues from the unauthorized use of personal information

116. Defendants' conduct lacks reasonable and legitimate justification in that Defendants have benefited from such conduct and practices while Plaintiff and the Class Members have been misled as to the nature and integrity of Defendants' services and have, in fact, suffered injury regarding the privacy and confidentiality of their personal information and the use of their device resources. Defendants' conduct offends public policy in California in connection with the Consumer Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to safeguard their own privacy interests, including California Civil Code, Section 1798.80.

117. In addition, Defendants' actions constitute an unfair practice in that Defendants knew, or should have known, that consumers care about the status of personal information regarding visited websites, GPS location and text privacy but were unlikely to be aware of the manner in which Defendants failed to fulfill their commitments with respect to the consumers' privacy.

118. Defendants' acts and practices were fraudulent within the meaning of the Unfair Competition Law because they were likely to mislead the consumers.

119. Defendants' practice of capturing, storing, and transferring highly detailed and personal records of consumers' incoming text messages, URLs of websites visited and GPS location histories, and storing such information in unencrypted form, is in violation of the Unfair Competition Law. Plaintiff and Class Members have suffered loss by reason of these

violations, including, violation to their right of privacy. Defendants exposed Plaintiff's and Class Members' personal information to any third party software or applications with log file access residing on their mobile devices without Plaintiff's or Class Members' consent or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members' mobile devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover, Plaintiff and Class Members had to pay unauthorized charges to their mobile devices for every hidden text message that was sent by Defendants.

FIFTH CAUSE OF ACTION

Violation of California's Computer Crime Law

Penal Code § 502 et seq.

Against All Defendants

120. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

121. The California Computer Crime Law, California Penal Code Section 502 regulates "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." A mobile device is a "computer system" as defined in Penal Code Section 502(b)(5) in that it contains electronic instructions, inputs and outputs data, performs functions including communication and data storage and retrieval.

122. Defendants violated California Penal Code § 502 by knowingly accessing, copying, using, making use of, interfering, and/or altering, data belonging to Plaintiff and Class Members: (1) in and from the State of California; (2) in the home states of the Plaintiff and Class Members; and (3) in the state in which the servers that provided the communication link between Plaintiff and Class Members and the applications they interacted with were located.

123. At all relevant times, Defendants had a business practice of accessing Plaintiff's and Class Members' mobile devices on a systematic and continuous basis in order to obtain mobile device data and to monitor and collect data related to their browsing habits, GPS locations and incoming text messages. Defendants accessed such data without notice to or

authorization from Plaintiff or Class Members.

124. Pursuant to California Penal Code § 502(b)(1), "Access means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network."

125. Pursuant to California Penal Code § 502(b)(6), "Data means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device."

126. Defendants have violated California Penal Code § 502(c)(1) by knowingly accessing and without permission, altering, and making use of data from Plaintiff's and Class Members' mobile devices in order to devise and execute business practices to deceive Plaintiff and Class Members into surrendering private electronic communications, and to wrongfully obtain valuable private data and device resources from Plaintiff and Class Members.

127. Defendants have violated California Penal Code § 502(c)(2) by knowingly accessing and without permission, taking, or making use of data from Plaintiff's and Class Members' mobile devices.

128. Defendants have violated California Penal Code § 502(c)(3) by knowingly and without permission, using and causing to be used Plaintiff's and Class Members' mobile computing devices' services and resources.

129. Defendants have violated California Penal Code section 502(c)(4) by knowingly accessing and, without permission, adding and/or altering the data from Plaintiff's and Class Members' computers, including application code installed on such computers.

130. Defendants have violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiff's and Class Members' mobile devices and mobile device systems.

131. Defendants has violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiff's and Class Members' mobile devices and mobile device systems.

132. California Penal Code § 502(j) states: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

133. Plaintiff and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy. Defendants exposed Plaintiff's and Class Members' personal information to any third party software or application with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members' mobile devices including battery power, cell phone memory, CPUs, and bandwidth. Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden text message that was sent by Defendants.

134. Plaintiff and Class Members have also suffered irreparable injury from these unauthorized acts of disclosure, to wit: their personal, private, and sensitive electronic data was obtained and used by Defendant. Due to the continuing threat of such injury, Plaintiff and Class Members have no adequate remedy at law, entitling Plaintiff and the Class to injunctive relief.

135. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy and depletion of valuable device resources.

136. As a direct and proximate result of Defendants' unlawful conduct within the meaning of California Penal Code § 502, Defendants have caused loss to Plaintiff and Class Members in an amount to be proven at trial. Plaintiff and Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

137. Plaintiff and the Class Members seek compensatory damages, in an amount to be proven at trial, and injunctive or other equitable relief.

SIXTH CAUSE OF ACTION

Violation of the California Invasion of Privacy Act

Penal Code § 630 et seq.

Against All Defendants

138. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

139. California Penal Code Section 630 provides, in part:

> Any person who, . . . or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable. . . .

140. At all relevant times, Defendants engaged in a business practice of accessing the mobile device data of the Plaintiff and Class Members without their authorization and consent and systematically logging and collecting their incoming text messages, URLs of websites viewed and GPS coordinates. Defendants made this personal data available to all third party software or applications with log file access on the mobile devices of Plaintiff and Class Members in an unencrypted form, without the consent or authorization of Plaintiff or Class Members.

141. On information and belief, Plaintiff and each Class Member, during one or more of their interactions on their mobile device, including receipt of text messages and URL browsing, communicated with one or more web entities based in California, or with one or more entities whose servers were located in California.

142. Communications from the California web-based entities to Plaintiff and Class Members were sent from California. Communications to the California web-based entities from Plaintiff and Class Members were sent to California.

143. Plaintiff and Class Members did not consent to any of the Defendants' actions in intercepting, reading, and/or learning the contents of their communications with such California-based entities.

144. Plaintiff and Class Members did not consent to any of the Defendants' actions in using the contents of their communications with such California-based entities.

145. Neither Defendant is a " public utility engaged in the business of providing communications services and facilities . . .."

146. The actions alleged herein by the Defendants were not undertaken "for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility."

147. The actions alleged herein by the Defendants were not undertaken in connection with "the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility."

148. The actions alleged herein by Defendants were not undertaken with respect to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

149. Defendants directly participated in intercepting, reading, and/or learning the contents of the communications between Plaintiff, Class Members and California-based web entities.

150. Alternatively, and of equal violation of the California Invasion of Privacy Act, Huawei aided, agreed with, and/or conspired with Carrier IQ to unlawfully do, or permit, or cause to be done all of the acts complained of herein.

151. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy. Defendants exposed Plaintiff's and Class Members' personal information to any third party software or application with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members'

mobile devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover, Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden text message that was sent by Defendants.

152. Unless restrained and enjoined, Defendants will continue to commit such acts. Pursuant to § 637.2 of the California Penal Code, Plaintiff and the Class have been injured by the violations of California Penal Code Section 631. Wherefore, Plaintiff, on behalf of himself and on behalf of a similarly situated Class of consumers, seeks damages and injunctive relief.

SEVENTH CAUSE OF ACTION

Violation of the Song-Beverly Warranty Act, California Civil Code §1792

Against All Defendants

153. Plaintiff incorporates by reference the allegations contained in all the paragraphs of this Complaint.

154. Huawei warranted to Plaintiff and Class Members in its "Manufacturer's Warranty" that the mobile devices would be free from defects for normal consumer usage for twelve months from the date of purchase.

155. Huawei by offering mobile devices in the marketplace represented and warranted to Plaintiff and Class Members that these devices did not cause personal information to be unreasonably and unexpectedly transferred to third parties.

156. Plaintiff and Class Members paid more for their mobile devices than they would have paid if Huawei disclosed the fact that the mobile devices were designed with defects, namely the privacy breach to Carrier IQ and any other third party software on the mobile device.

157. A reasonable consumer would, and Plaintiff and Class Members did expect that, if Huawei mobile devices were subject to defects such as those identified above, Huawei would disclose these material facts and Plaintiff and Class Members would not have purchased these devices.

158. Plaintiff and Class Members paid premiums for Huawei mobile devices because they reasonably believed the devices were designed to employ reasonable security in their

operation.

159. Huawei's failure to meet the specifications of the mobile devices violates the express and implied warranties under the Song-Beverly Warranty Act, California Civil Code §1792 et.seq.

160. Moreover, Huawei asserts that disabling the Carrier IQ software on a mobile device voids the Huawei Warranty. Plaintiff and Class Members are therefore forced to induce breach of the Huawei Warranty by disabling the Carrier IQ software to protect their personal information.

161. Plaintiff and Class Members who purchased the mobile devices are entitled to a refund of the purchase price.

EIGHTH CAUSE OF ACTION

Texas Deceptive Trade Practices Act, Business and Commerce Code § 17.41 et seq.

Against All Defendants

162. Plaintiff incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

163. Plaintiff is a "consumer" under the Texas Deceptive Trade Practices Act as he purchased and used a Huawei mobile device that had been preinstalled with the Carrier IQ tracking program.

164. Defendants are proper "persons" or defendants under the Texas Deceptive Trade Practices Act, who either used or employed false, misleading, deceptive or unconscionable acts or practices, or were directly connected with the transaction with Plaintiff.

165. Defendants committed multiple violations and wrongful acts under the Texas Deceptive Trade Practices Act, including the following: making or committing, false, misleading or deceptive acts and/or practices, including but not limited to violations of Tex. Business & Commerce Code § 17.46(b) (3), (5), (7), (9), (20), and (24). Defendants committed misleading and unconscionable acts in connection with the sale of mobile devices installed or updated with IQ Agent to Plaintiff and Class Members, and the subsequent tracking and

logging of Plaintiff's and Class Members' confidential, unencrypted through IQ Agent without notice or consent. In carrying out these acts, Defendants depleted Plaintiff's and Class Members' mobile device resources without notice to or consent from Plaintiff or Class Members. Plaintiff and Class Members relied on Defendants' acts and/or practices to their detriment.

166. Plaintiff and Class Members will show that the violation and actions of Defendants were a producing cause of their damages. Defendants exposed Plaintiff's and Class Members' personal information to any third party software or applications with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of Plaintiff's and Class Members' mobile device resources including battery power, cell phone memory, CPUs, and bandwidth. Moreover, Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden text message that was sent by Defendants.

167. Plaintiff will show that the violations and actions of Defendants were done intentionally or knowingly, entitling Plaintiff to treble damages.

168. Plaintiff will show that the violations and actions of Defendants entitle him to reasonable and necessary attorney's fees under the Texas Deceptive Trade Practices Act, specifically Tex. Business & Commerce Code § 17.50(d).

NINTH CAUSE OF ACTION

Breach of Express Warranty

Against Defendant Huawei

169. Plaintiff incorporates by reference the allegations contained in all the paragraphs of this Complaint.

170. Huawei warranted to Plaintiff and Class Members in its "Manufacturer's Warranty" that the mobile devices would be free from defects for normal consumer usage for twelve months from the date of purchase.

171. Huawei sold mobile devices to Plaintiff and Class Members that were defective

because they caused personal information to be unreasonably and unexpectedly viewed and collected by Carrier IQ and other third party software and applications. The devices also were subject to depletion of resources through the IQ Agent software which depleted those resources without notice to or authorization from Plaintiff or Class Members.

172. Plaintiff and Class Members paid more for their mobile devices than they would have paid if Huawei disclosed the fact that the mobile devices were designed with defects, namely the privacy breach and depletion of mobile device resources.

173. A reasonable consumer would, and Plaintiff and Class Members did expect that, if Huawei mobile devices were subject to defects such as those identified above, Huawei would disclose these material facts and Plaintiff and Class Members would not have purchased these devices.

174. Plaintiff and Class Members paid premiums for Huawei mobile devices because they reasonably believed the devices were designed to employ reasonable security in their operation.

175. Huawei's failure to provide to Plaintiff and Class Members a mobile device that is not defective is a violation of Huawei's express Warranty.

176. Moreover, Huawei asserts that disabling the Carrier IQ software on a mobile device voids the Huawei Warranty. Plaintiff and Class Members are therefore forced by Huawei to induce breach of the Huawei Warranty by disabling the Carrier IQ software to protect their personal information.

177. Plaintiff and Class Members who purchased the mobile devices are entitled to a refund of the purchase price.

TENTH CAUSE OF ACTION

Breach of Implied Warranty

Against Defendant Huawei

178. Plaintiff incorporates by reference the allegations contained in all the paragraphs of this Complaint.

179. Huawei by offering mobile devices in the marketplace represented and

warranted to Plaintiff and Class Members that these devices would be free from defects for normal consumer usage and would not cause personal information to be unreasonably and unexpectedly transferred to third parties.

180. Huawei sold mobile devices to Plaintiff and Class Members that were defective because they caused personal information to be unreasonably and unexpectedly viewed and collected by Carrier IQ and other third party software and applications. The devices also were subject to depletion of resources through the IQ Agent software which depleted those resources without notice to or authorization from Plaintiff or Class Members.

181. Plaintiff and Class Members paid more for their mobile devices than they would have paid if Huawei disclosed the fact that the mobile devices were designed with defects, namely the privacy breach and depletion of mobile device resources.

182. A reasonable consumer would, and Plaintiff and Class Members did expect that, if Huawei mobile devices were subject to defects such as those identified above, Huawei would disclose these material facts and Plaintiff and Class Members would not have purchased these devices.

183. Plaintiff and Class Members paid premiums for Huawei mobile devices because they reasonably believed the devices were designed to employ reasonable security in their operation.

184. Huawei's failure to provide to Plaintiff and Class Members are therefore forced by Huawei to induce breach of the Huawei Warranty by disabling the Carrier IQ software to protect their personal information.

185. Huawei by offering mobile devices in the marketplace represented and warranted to Plaintiff and Class Members that these devices would be free from defects for normal consumer usage and would not cause personal information to be unreasonably and unexpectedly transferred to third parties.

186. Huawei sold mobile devices to Plaintiff and Class Members that were defective because they caused personal information to be unreasonably and unexpectedly viewed and collected by Carrier IQ and other third party software and applications. The devices also were

subject to depletion of resources through the IQ Agent software which depleted those resources without notice to or authorization from Plaintiff or Class Members.

187. Plaintiff and Class Members paid more for their mobile devices than they would have paid if Huawei disclosed the fact that the mobile devices were designed with defects, namely the privacy breach and depletion of mobile device resources.

188. A reasonable consumer would, and Plaintiff and Class Members did expect that, if Huawei mobile devices were subject to defects such as those identified above, Huawei would disclose these material facts and Plaintiff and Class Members would not have purchased these devices.

189. Plaintiff and Class Members paid premiums for Huawei mobile devices because they reasonably believed the devices were designed to employ reasonable security in their operation.

190. Huawei's failure to provide to Plaintiff and Class Members a mobile device that is not defective is a violation of Huawei's implied Warranty.

191. Plaintiff and Class Members who purchased the mobile devices are entitled to a refund of the purchase price.

ELEVENTH CAUSE OF ACTION

Negligence

Against All Defendants

192. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

193. Carrier IQ and Huawei owed a duty of care to Plaintiff and Class Members.

194. Carrier IQ and Huawei breached their duty by negligently designing IQ Agent and preinstalling or uploading it to Plaintiff's and Class Members' mobile devices without any notice or authorization so that Defendants could acquire personal information without Plaintiff's and Class Members' knowledge or permission. Defendants also negligently made this confidential data available to any software or application with log file access on the mobile device, in an unencrypted format. Defendants also negligently depleted Plaintiff's and Class

Members' mobile device resources.

195. Carrier IQ and Huawei failed to fulfill their own commitments to Plaintiff and Class Members, and further failed to fulfill even the minimum duty of care to protect Plaintiff's and Class Members' personal information, privacy rights, security, and device resources.

196. Huawei's unencrypted storage of Plaintiff's and Class Members' on the mobile device log file and Carrier IQ servers was negligent.

197. Plaintiff and Class Members were harmed as a result of Carrier IQ's breaches of its duty, and Carrier IQ proximately caused such harms.

198. Huawei's failure to fulfill its commitments included allowing Carrier IQ's practice of preinstalling IQ Agent on Huawei mobile device users' devices without notice or authorization and then permitting Carrier IQ to collect unencrypted data in the log file and make it available, unencrypted, to third party software and applications with log file access on the devices. Huawei engaged in these activities without notice to or consent from Plaintiff and Class Members.

199. Huawei's preinstallation or upload of IQ Agent and unauthorized use of Plaintiff's and Class Members' confidential information without notice to or consent from Plaintiff or Class Members was negligent.

200. Defendants exposed Plaintiff's and Class Members' personal information to any third party software with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of their mobile devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover, Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden text message that was sent by Carrier IQ.

201. Plaintiff and Class Members were harmed as a result of Defendants' breaches of their duty, and Defendants proximately caused such harms.

///

TWELFTH CAUSE OF ACTION

Trespass to Personal Property/Chattels

Against All Defendants

202. Plaintiff incorporates by reference all paragraphs previously alleged herein.

203. The common law prohibits the intentional intermeddling with personal property, including a mobile device, in possession of another which results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

204. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiff and Class Members, Defendants dispossessed Plaintiff and Class Members from use and/or access to their mobile devices, or parts of them. Further, these acts impaired the use, value, and quality of Plaintiff's and Class Members' mobile devices. Defendants' acts constituted an intentional interference with the use and enjoyment of their mobile devices. By the acts described above, Defendants have repeatedly and persistently engaged in trespass to personal property in violation of the common law.

205. Without Plaintiff's and Class Members' consent, or in excess of any consent given, Defendants knowingly and intentionally accessed Plaintiff's and Class Members' property, thereby intermeddling with Plaintiff's and Class Members' right to possession of the property and causing injury to Plaintiff and the members of the Class.

206. Defendants engaged in deception and concealment in order to gain access to Plaintiff's and Class Members' mobile devices.

207. Defendants undertook the following actions with respect to Plaintiff's and Class Members' mobile devices:

208. Defendants accessed and obtained control over the users' mobile device;

209. Defendants caused the installation of code on the hard drives of the mobile devices;

210. Defendants programmed the operation of its code to circumvent the mobile device owners' privacy and security controls, to remain beyond their control, and to continue

to function and operate without notice to them or consent from Plaintiff and Class Members;

211. Defendants obtained users' personal information by logging confidential data in the log file;

212. Defendants utilized users' mobile device resources as part of logging confidential data; and

213. Defendants used the log file data to obtain information about the mobile browsing activities of the mobile device without the user's consent, and outside of the control of the owner of the mobile device.

214. All these acts described above were acts in excess of any authority any user granted Defendants when the user purchased the Huawei mobile device that had IQ Agent preinstalled or updated on the device without the user's consent or knowledge. By engaging in deception and misrepresentation, whatever authority or permission Plaintiff and Class Members may have granted to Defendants was exceeded.

215. Defendants' installation and operation of its program used, interfered, and/or intermeddled with Plaintiff's and Class Members' mobile devices. Such use, interference and/or intermeddling was without Plaintiff's and Class Members' consent or, in the alternative, in excess of Plaintiff's and Class Members' consent.

216. Defendants' installation and operation of its program constitutes trespass, nuisance, and an interference with Plaintiff's and Class Members' chattels, to wit, their mobile devices.

217. Defendants' installation and operation of the Carrier IQ program impaired the condition and value of Plaintiff's and Class Members' mobile devices.

218. Defendants' trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiff and Class Members Defendants exposed Plaintiff's and Class Members' personal information to any third party software with log file access residing on their mobile devices without Plaintiff's or Class Members' permission or knowledge, and in an unencrypted form. Plaintiff and Class Members were damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members' mobile devices including battery power,

cell phone memory, CPUs, and bandwidth. Plaintiff and Class Members had unauthorized charges to their mobile devices for every hidden text message that was sent by Carrier IQ.

219. As a direct and proximate result of Defendants' trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiff's and Class Members' property, Defendants have injured and impaired Plaintiff and Class Members in the condition and value of Plaintiff's Class Members' mobile devices, as follows:

(a) By consuming the resources of and/or degrading the performance of Plaintiff's and Class Members' mobile devices (including space, memory, processing cycles, Internet connectivity, and unauthorized use of their bandwidth);

(b) By diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiff's and Class Members' mobile devices;

(c) By devaluing, interfering with, and/or diminishing Plaintiff's and Class Members' possessory interest in their mobile devices;

(d) By altering and/or controlling the functioning of Plaintiff's and Class Members' mobile devices;

(e) By infringing on Plaintiff's and Class Members' right to exclude others from their mobile devices;

(f) By infringing on Plaintiff's and Class Members' right to determine, as owners of/or their mobile devices, which programs should be installed and operating on their mobile devices;

(g) By compromising the integrity, security, and ownership of Class Members' mobile devices; and

(h) By utilizing Plaintiff's and Class Members' mobile device resources without notice or consent.

THIRTEENTH CAUSE OF ACTION

Unjust Enrichment

Against All Defendants

220. Plaintiff incorporates by reference the allegations contained in all of the

paragraphs of this complaint.

221. By engaging in the conduct described in this Complaint, Defendants have knowingly obtained benefits from the Plaintiff and Class Members under circumstances that make it inequitable and unjust for Defendants to retain them.

222. Plaintiff and the Class have conferred a benefit upon the Defendants who have, directly or indirectly, received and retained the confidential information of Plaintiff and Class Members as set forth herein. Defendants have received and retained information that is otherwise private, confidential, and not of public record, and/or have received revenue from the provision, use, and or trafficking in the sale of such information.

223. Defendants appreciate and/or have knowledge of said benefit.

224. Under principles of equity and good conscience, Defendants should not be permitted to retain the information and/or revenue that they acquired by virtue of their unlawful conduct. All funds, revenue, and benefits received by them rightfully belong to Plaintiff and the Class, which the Defendants have unjustly received as a result of their actions.

225. Plaintiff and Class Members have no adequate remedy at law.

226. Defendants have received a benefit from Plaintiff and Class Members and Defendants have received and retained money or other benefits from third parties as a result of sharing Plaintiff's and Class Members' confidential information of Plaintiff and Class Members without Plaintiff's or Class Members' knowledge or consent as alleged in this Complaint.

227. Plaintiff and Class Members did not expect that Defendants would seek to gain commercial or business advantage from third parties by using their personal information without their knowledge or consent.

228. Defendants knowingly used Plaintiff's and Class Members' confidential information without their knowledge or consent to gain commercial advantage from third parties and had full knowledge of the benefits they have received from Plaintiff and Class Members. If Plaintiff and Class Members had known Defendants were not keeping their confidential information from third-parties, they would not have consented and Defendants

would not have gained commercial or business advantage from third parties.

229. Defendants will be unjustly enriched if Defendants are permitted to retain the money or other benefits paid to them by third parties, or resulting from the commercial or business advantage they gained, in exchange for Plaintiff's and Class Members' confidential information.

230. Defendants should be required to provide restitution of all money obtained from their unlawful conduct.

231. Plaintiff and the Members of the Class are entitled to an award of compensatory and punitive damages in an amount to be determined at trial or to be imposition of a constructive trust upon the wrongful revenues and/or profits obtained by and benefits conferred upon Defendants as a result of the wrongful actions as alleged in this complaint.

232. Plaintiff and the Class have no remedy at law to prevent Defendants from continuing the inequitable conduct alleged in this complaint and the continued unjust retention of the money and/or benefits Defendants received from third parties.

FOURTEENTHCAUSE OF ACTION

Conversion

Against All Defendants

233. Plaintiff incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

234. Plaintiff's and Class Members' mobile device data, including but not limited to their incoming text messages, URLs of websites viewed and GPS coordinates, was viewed by Defendants and made available to third party software and applications with log file permission to collect confidential, unencrypted data about Plaintiff's and Class Members' mobile device activities. Such property, owned by the Plaintiff and Class Members, is valuable to the Plaintiff and Class Members.

235. Plaintiff's and Class Members' mobile devices use battery power, cell phone memory, CPUs, and bandwidth. Defendants' activities, made the basis of this action, used without notice or authorization, such battery power, memory, CPU and bandwidth for purposes

not contemplated and not agreed to by Plaintiff and Class Members when they purchased their Huawei mobile devices. Such property, owned by Plaintiff and Class Members, is valuable to Plaintiff and Class Members. Plaintiff and Class Members were damaged by Defendants' unauthorized use of Plaintiff's and Class Members' battery power, cell phone memory and CPUs, as well as bandwidth. Moreover, Defendants utilized Plaintiff's and Class Members' limited text messages in order to send secret and unauthorized instructions to their mobile devices. Plaintiff and Class Members paid unauthorized charges for every hidden text message that was sent by Defendants.

236. Defendants unlawfully exercised dominion over said property and thereby converted Plaintiff's and Class Members' property.

237. Plaintiff and Class Members were damaged by Defendants' actions.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for judgment against Defendants as follows:

A. Certify this case as a Class action on behalf of the Classes defined above, appoint Plaintiff as a Class representative, and appoint his counsel as Class counsel;

B. Declare that the actions of Defendants, as set out above, violate the claims alleged;

C. Award injunctive and equitable relief including, *inter alia*: (i) prohibiting Defendants from engaging in the acts alleged above; (ii) requiring Defendants to disgorge all of their ill-gotten gains to Plaintiff and Class Members, or to whomever the Court deems appropriate; (iii) requiring Defendants to delete all data surreptitiously or otherwise collected data through the acts alleged above; (iv) requiring Defendants to provide Plaintiff and Class Members a means to easily and permanently decline any participation in any data collection activities; (v) awarding Plaintiff and Class Members full restitution of all benefits wrongfully acquired by Defendants by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by

unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendants;

D. Award damages, including statutory damages where applicable, to Plaintiff and Class Members in an amount to be determined at trial;

E. Award restitution against Defendants for all money to which Plaintiff and the Classes are entitled in equity;

F. Restrain Defendants, their officers, agents, servants, employees, and attorneys, and those in active concert or participation with them from continued access, collection, and transmission of Plaintiff's and Class Members' confidential user data via preliminary and permanent injunction;

G. Award Plaintiff and the Classes:

(a) Compensatory damages sustained by Plaintiff and all others similarly situated as a result of Defendants' unlawful acts and conduct;

(b) Restitution, disgorgement and/or other equitable relief as the Court deems proper;

(c) Plaintiff's reasonable litigation expenses and attorneys' fees;

(d) Pre- and post-judgment interest, to the extent allowable;

(e) Statutory damages, including punitive damages; and

(f) Permanent injunction prohibiting Defendants from engaging in the conduct and practices complained of herein.

For such other and further relief as this Court may deem just and proper.

Dated this 21st day of March, 2012.

By:

STRANGE & CARPENTER

Brian R. Strange (Cal. Bar. No. 103252)
LACounsel@earthlink.net
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Telephone: (310) 207-5055
Facsimile: (310) 826-3210

Law Office of Joseph H. Malley
Joseph H. Malley (not admitted)
malleylaw@gmail.com
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

Counsel for Plaintiff and the Proposed Class

JURY TRIAL DEMAND

The Plaintiff hereby demands a trial by jury of all issues so triable.

Dated this 21st day of March, 2012.

By:

STRANGE & CARPENTER

Brian R. Strange (Cal. Bar. No. 103252)
LACounsel@earthlink.net
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Telephone: (310) 207-5055
Facsimile: (310) 826-3210

Law Office of Joseph H. Malley
Joseph H. Malley (not admitted)
malleylaw@gmail.com
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

Counsel for Plaintiff and the Proposed Class