

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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 (*pro hac vice* pending)
malleylaw@gmail.com
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

Attorneys for Plaintiffs

**IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION—SANTA ANA**

LISA CLARK, FELIPE GARCIA and
ROBERT SPRADLEY; individuals, on
behalf of themselves and others similarly
situated,

Plaintiffs,

v.

CARRIER IQ, INC., a Delaware
Corporation; SAMSUNG
ELECTRONICS AMERICA, INC., and
SAMSUNG
TELECOMMUNICATIONS
AMERICA, LLC

Defendant.

CASE No. **SACV11-01899 AG (JPRx)**

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

FILED

2011 DEC -8 PM 3: 50

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
SANTA ANA

BY _____

- 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
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. Plaintiffs Lisa Clark, Felipe Garcia and Robert Spradley (collectively, "Plaintiffs"), by and through their attorneys Strange & Carpenter, and Law Office of Joseph H. Malley, P.C., brings this action on behalf of themselves and all others similarly situated, against Carrier IQ, Inc. ("Carrier IQ"), Samsung Electronics America, Inc. and Samsung Telecommunications America, CLL (collectively with Samsung Electronics America, Inc., "Samsung") (collectively with Carrier IQ, "Defendants"). Plaintiffs' allegations as to themselves and their own actions, as set forth herein, are based upon their 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.

1 **I. NATURE OF THE ACTION**

2 2. Plaintiffs brings this consumer Class Action lawsuit pursuant to
3 Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of
4 themselves and a proposed class of similarly situated consumers ("Class
5 Members") who purchased a Samsung mobile device on which Carrier IQ's
6 software, "IQ Agent," was installed, without notice or consent of Plaintiffs. This
7 IQ Agent software was designed by Carrier IQ and customized by Samsung in
8 order to log and collect confidential, unencrypted user data including but not
9 limited to (1) the contents of incoming text messages; (2) the URLs of websites
10 visited by the user; and (3) the user's GPS coordinates; among other private and
11 personally-identifying data. IQ Agent records this confidential data on a user's
12 mobile device in an unencrypted format so that *any* device software or
13 applications with log file permission can access and review it. Carrier IQ and
14 Samsung also have access to this confidential data and can transmit the data from
15 a user's mobile device to remote servers at any time via hidden "text requests"
16 sent to a user's mobile device by Carrier IQ, Samsung or other authorized third
17 parties. IQ Agent logs the hidden text requests and the confidential data silently
18 so that a user has no idea that data is being collected and transmitted. IQ Agent is
19 preinstalled on Samsung's mobile devices so that data logging begins the
20 moment a user purchases and turns on the device, without notice to or consent
21 from the user. Because the software is preinstalled by Samsung and runs as part
22 of the device operating system, data is automatically collected and can be
23 transmitted via wireless internet or other means, even if the device user has no
24 carrier contract and the mobile device is not connected to a mobile network.
25 Finally, IQ Agent runs continuously and depletes resources on the mobile device
26 without notice to or authorization of the user, even when the mobile device is not
27 being used. The resources depleted by IQ Agent without notice or authorization
28 include (1) battery power; (2) device memory; (3) CPU; (4) bandwidth; and (5)

1 text messages. A user cannot stop the IQ Agent software from running under any
2 circumstances, and a user is unable to remove IQ Agent from the device without
3 voiding the manufacturer's warranty.

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

16 4. Samsung manufactured and sold to Plaintiffs and Class Members
17 without notice, a defective product that included IQ Agent, specially customized
18 by Samsung for use on its mobile device. Samsung acted individually, and in
19 concert with, Carrier IQ to gain unauthorized access to, log, collect, and transmit
20 Plaintiffs' and Class Members' confidential, unencrypted data and to provide
21 third-party access to this data. IQ Agent is a native Samsung application that was
22 installed on Samsung mobile devices with the knowledge of Samsung.

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

26 6. Carrier IQ individually, and in concert with Samsung has been
27 systematically engaged in and facilitated a covert operation of logging and
28 tracking Plaintiffs' and Class Members' confidential, unencrypted user data and

utilizing Plaintiffs' 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

1 \$5,000,000 and minimal diversity exists.

2 8. Venue is proper in this District under 28 U.S.C. §1391(b) and (c)
3 against Defendants. Although Carrier IQ purports to exist as a separate and
4 independent entity, facts show that it has an incestuous business relationship with
5 associated entities. Its operations, management and infrastructure are in fact
6 closely linked with the company Core Mobility, Inc. ("Core Mobility") and its
7 Orange County-based parent company, Smith Micro Software, Inc. ("Smith
8 Micro"). Carrier IQ and Core Mobility are both founded by the same parties,
9 arise from patents by the same inventor, and share offices next door in Mountain
10 View, California. An IP address linked to the hostname
11 "collector.argus.coremobility.com" actually goes to the hostname
12 "collector.argus.carrieriq.com." In other words, data one expects to be going to
13 Carrier IQ could be transmitted to Core Mobility. Additionally Core Mobility
14 owns what is believed to be a majority of shares in Carrier IQ. For all intents and
15 purposes, Core Mobility and Carrier IQ are assimilated.

16 9. Core Mobility is a wholly-owned subsidiary of Smith Micro, a
17 software company based in Aliso Viejo, California. According to Smith Micro's
18 2009 10K, Smith Micro acquired Core Mobility in its entirety and "assimilate[d]
19 the operations, products and personnel of [Core Mobility] and train[ed],
20 retrain[ed] and motivate[d] key personnel from the acquired business."

21 10. Core Mobility's telephone service identifies the company as "Smith
22 Micro Software" and Core Mobility executive employees at the Smith Micro
23 office and have Smith Micro titles. It appears that Core Mobility does not have its
24 own office or personnel apart from Smith Micro, and its operations have been
25 completely assimilated into Smith Micro. It also appears that Core Mobility and
26 Carrier IQ are separate entities in name only so that Carrier IQ is also managed
27 by Smith Micro in this District.

28 11. 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. Samsung conducts business in California and engaged in the acts alleged herein in California.

12. 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.

III. PARTIES

13. Plaintiff Lisa Clark ("Clark") is a citizen and resident of Ardmore, Oklahoma, (Carter County). On information and belief, Clark incorporates all allegations within this complaint. Clark is a representative of the class ("Class"), as defined within the Class Allegations. In or around 2011, Clark purchased a Samsung Galaxy that was preinstalled or updated with IQ Agent, and used such mobile device on one or more occasions during the class period in Oklahoma.

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

1 application launch list on Clark's device.

2 15. Plaintiff Felipe Garcia ("Garcia") is a citizen and resident of Dallas,
3 Texas (Dallas County). On information and belief, Garcia incorporates all
4 allegations within this complaint. Garcia is a representative of the Class, as
5 defined within the Class Allegations. In or around November 2011, Garcia
6 purchased a Samsung Galaxy S II Epic Touch mobile device that was preinstalled
7 with IQ Agent, and used such mobile device on one or more occasions during the
8 class period in Texas.

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

20 17. Plaintiff Robert Spradley ("Spradley") is a citizen and resident of
21 Amarillo, Texas (Potter County). On information and belief, Spradley
22 incorporates all allegations within this complaint. Spradley is a representative of
23 the Class, as defined within the Class Allegations. In or around December 2010,
24 Spradley purchased a Samsung Galaxy Epic 4G mobile device that was
25 preinstalled or updated with IQ Agent, and used such mobile device on one or
26 more occasions during the class period in Texas.

27 18. Spradley was not aware that IQ Agent was installed on his Samsung
28 device, and was not aware that every time he used his Samsung device, IQ Agent

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

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

15 20. Samsung Electronics America, Inc. is a New York corporation with
16 its principal place of business located at 105 Challenger Road, Ridgefield Park,
17 New Jersey 07660. Samsung Electronics America, Inc. does business throughout
18 the United States, and in particular, does business in the State of California and in
19 this County.

20 21. Samsung Telecommunications America, Inc. is a Delaware
21 corporation with its principal place of business located at 1301 East Lookout
22 Drive, Richardson, Texas 75081. Samsung Telecommunications America, Inc.
23 does business throughout the United States, and in particular, does business in the
24 State of California and in this County.

25 **IV. PLAINTIFFS' EXPERIENCE**

26 22. At all relevant times herein, Plaintiffs were and are residents of
27 Oklahoma and Texas. During the class period, Plaintiffs owned and operated one
28 or more Samsung mobile devices installed with IQ Agent without Plaintiffs'

1 knowledge.

2 23. On one or more occasions during the class period, Plaintiffs
3 accessed and used their Samsung mobile devices to receive text messages and
4 visit websites in their cities of residence and elsewhere.

5 24. During the relevant class period, the IQ Agent software was
6 "hidden" and did not appear on application launch menu on Plaintiffs' Samsung
7 mobile devices. During the relevant class period, Plaintiffs were unaware that IQ
8 Agent populated and logged incoming text messages, visited URLs and GPS
9 location data on their device log files. Plaintiffs were also unaware that this
10 confidential data was available, unencrypted, to all software and programs with
11 log file permission running on their devices. Additionally, they were unaware
12 that IQ Agent had the mechanisms to, and did, transmit user data from Plaintiffs'
13 devices to remote servers via periodic scheduling, WAP push requests, and text
14 requests.

15 25. During the relevant class period, IQ Agent, customized in part by
16 Samsung, was "hidden" and did not appear on the launch list of applications and
17 software installed on Plaintiffs' Samsung mobile devices.

18 26. In or around November 2011, Plaintiffs became aware of
19 information related to the tracking activities of Carrier IQ and Samsung.

20 27. Plaintiffs' mobile devices revealed that the IQ Agent software
21 resided on their device without notice to Plaintiffs or authorization from
22 Plaintiffs.

23 28. Plaintiffs consider information about their received text messages,
24 visited websites and GPS location to be in the nature of confidential and personal
25 information that they protect from disclosure, including by controlling their
26 mobile device's privacy settings for acceptance or rejection. Plaintiffs were not
27 made aware by Defendants of the existence of IQ Agent on their mobile devices
28 or the logging, collection and transmission of their mobile device data.

1 29. Plaintiffs also consider their device battery power, device memory,
2 CPU, bandwidth and text messages to be valuable personal property that they
3 protect from unauthorized use by third parties, including by controlling what
4 software and applications have access to those resources. Plaintiffs were not
5 made aware by Defendants of the existence of IQ Agent on their mobile devices
6 or the depletion of their device battery power, device memory, CPU, bandwidth
7 and text messages by that software.

8 30. It is Plaintiffs' belief that The Carrier IQ software, customized in
9 part by Samsung, was logging, collection and transmission of confidential user
10 data on their mobile devices permitted one or more objects within their mobile
11 devices to be used for tracking and analysis by Defendants and/or third parties,
12 thus their mobile device data was obtained in an effort to monitor and profile
13 their mobile device activities. Plaintiffs did not receive notice of the installation
14 of a tracking identifier, did not consent to its installation, and did not want a
15 tracking identifier to be installed on their mobile device. Moreover, Plaintiffs did
16 not authorize Defendants to log, collect, transmit, or store their confidential
17 mobile device data without notice or express consent. Such software was running
18 on Plaintiffs mobile device and collecting and transmitting Plaintiffs data without
19 notice or authorization, utilizing Plaintiffs battery power, device memory, CPU,
20 bandwidth and limited text messages without notice or authorization, even when
21 Plaintiffs stopped actively using the device.

22 31. In selecting the Samsung mobile device over the service and goods
23 of other competing mobile device manufacturers, Plaintiffs reasonably expected
24 that their confidential user data would not be accessed, logged and transmitted to
25 third parties without their knowledge and consent. They also reasonably expected
26 that their mobile device resources would not be depleted without their knowledge
27 or control.

28 32. Had Plaintiffs known that the Samsung devices they purchased

1 would include software that provided third party access to their confidential user
2 data and their mobile device resources without notice to or authorization by
3 Plaintiffs, Plaintiffs would have not purchased those devices.

4 33. Plaintiffs were harmed by Defendants' practices, including but not
5 limited to the following:

6 (a) Costs to purchase the defective Samsung mobile device;

7 (b) Violations of Plaintiffs' legally protected federal, state and
8 common law rights of privacy, especially related to unencrypted logging,
9 storage and transmission of Plaintiffs' confidential user data;

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

12 (d) Time and expense to repair Plaintiffs' mobile devices and
13 remedy the impaired operability caused by the Defendants;

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

16 (f) Financial harm by the Defendants' unauthorized use of
17 Plaintiffs' and mobile device resources during the unauthorized process of
18 logging and transmitting user data.

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

1 35. Defendants' business practices unfairly wrested from Plaintiffs
2 control over their user data privacy and control over their device resources.
3 Defendants' logging, collection, and unencrypted disclosure of Plaintiffs'
4 confidential user data violates user expectations, diminishes user privacy, and
5 contradicts the Manufacturer's Warranty. Defendants caused harm and damages
6 to Plaintiffs' finite device resources, thus preventing Plaintiffs to use the devices
7 for their intended purposes and resulting in instability issues.

8 **V. COMMON EXPERIENCES BETWEEN PLAINTIFFS AND CLASS**
9 **MEMBERS**

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

13 (a) Plaintiffs and Class Members are individuals in the United
14 States who purchased and used a Samsung mobile device that had IQ Agent
15 software installed and customized by Samsung, without notice or consent;

16 (b) Samsung a mobile device manufacturer had entered into a
17 legally binding contract with Carrier IQ to host the IQ Agent software on its
18 mobile device.

19 (c) Carrier IQ was aware that Samsung had preinstalled IQ
20 Agent on Plaintiffs' and Class Members' mobile devices, aware. That Samsung
21 had customized y IQ Agent, aware that IQ Agent was "hidden" and did not
22 appear in the launch list of applications installed on Plaintiffs' and Class
23 Members' mobile devices;

24 (d) Plaintiffs and Class Members accessed and used their
25 Samsung mobile devices that had the preinstalled or uploaded IQ Agent
26 software application;

27 (e) Carrier IQ collected confidential user data from Plaintiffs'
28 and Class Members' mobile devices without the consent of, or notice to,

1 Plaintiffs and Class Members;

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

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

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

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

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

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

25 (l) Carrier IQ obtained individually, and in concert with
26 Samsung, Plaintiffs' and Class Members' confidential user data, derived, in
27 whole or part, from its monitoring the mobile device activities of Plaintiffs and
28 Class Members. This sensitive information includes but is not limited to

1 incoming text messages, visited URLs and GPS coordinates;

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

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

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

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

19 (q) Defendants depleted Plaintiffs' and Class Members' mobile
20 device resources while running the IQ Agent software, including the device
21 battery power, device memory, CPU, bandwidth and text messages.

22 37. Plaintiffs and Class Members involved with the Defendants were
23 harmed by Defendants' practices, including but not limited to the following:

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

28 (b) Financial Harm due to the costs to purchase the defective

1 Samsung mobile device;

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

4 (d) Financial Harm due to the time and expense to repair
5 Plaintiffs' mobile devices and remedy the impaired operability caused by the
6 Defendants;

7 (e) Financial Harm due to the loss of property due to the
8 inability to re-sell Plaintiffs' and Class Members' mobile devices due to the
9 Carrier IQ application;

10 (f) Financial Harm due to the loss of property due to the
11 unauthorized access and use of Plaintiffs' and Class Members' confidential user
12 data, depriving Plaintiffs and Class Members of such possession and use;

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

17 VI. FACTUAL ALLEGATIONS

18 A. Background

19 38. On October 26, 1999 the Wireless Communication and Public Act of
20 1999 was enacted and became known as the "e911 Act." It was an amendment to
21 the Telecommunication Act of 1996. The purpose of the bill was to promote and
22 enhance public safety through the use of 911 as universal assistance number. The
23 Federal Law mandated that mobile phones be embedded with a Global
24 Positioning System ("GPS") chip, which could calculate a user's coordinates to
25 within a few yards by receiving signals from satellites. This law enacted to aid
26 those in harm's way, resulted in the computing industry developing hardware
27 and software to assist in the development of this technology or mobile devices
28 provided Carrier IQ the impetus to originate a business plan to take advantage of

1 the benefit of embedded GPS chips in all mobile phones for its own commercial
2 benefit:

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

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

15 39. Carrier IQ's software is reportedly installed in excess of one hundred
16 and fifty million (150,000,000) mobile devices, including mobile devices
17 manufactured by Samsung. These devices installed with IQ Agent inherently
18 defective, and Defendants falsely advertised, marketed and distributing these
19 mobile devices, without disclosure of the material facts about the defect,
20 misrepresenting the performance of the devices, violating express and implied
21 warranties, thus rendering the mobile devices unable to be used for their intended
22 purposes. Such activities resulted in a pattern of covert mobile device
23 surveillance, wherein Defendants installed IQ Agent on Plaintiffs' and Class
24 Members' mobile device without authorization and consent, thereby committing
25 unauthorized access, collection, storage, and use of, the mobile device and data
26 derived from the Plaintiffs' and Class Members' use of the mobile devices and
27 transmitting information, code, and commands to collect, monitor, and remotely
28 store non-anonymized Plaintiffs' and Class Members' confidential mobile device

1 data. Defendants unauthorized access of this confidential, unencrypted data also
2 allowed access to *all* software and applications with log file access so that
3 Plaintiffs' and Class Members' data could be transmitted by multiple unknown
4 parties at any time, *like a pac-man creeping 150 million mobile phones and*
5 *"calling home."*

6 40. The Samsung-version of the software, IQ Agent, is currently
7 preinstalled by Samsung on its Carrier IQ-enabled mobile devices and was also
8 installed via software updates on older Samsung devices.

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

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

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

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

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

26 43. During the use of a mobile device in a mobile communication
27 network, parameter data defining conductors associated with the mobile device
28 and operation is generated. The mobile device also generates event data defining

1 events of the mobile device for the associated mobile user. Such events are
2 referred to as "Trigger points."

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

9 45. Carrier IQ's patent for "data collection associated with components
10 and services of a wireless communication network" explains the breadth of this
11 data collection,

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

20 <http://www.faqs.org/patents/app/20110106942> (last accessed December 2,
21 2011).

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

1 based on network .

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

6 48. Mobile Internet advertising currently consists of streaming graphic
7 files, in real time, into content rendered by a user's mobile device browser.

8 Mobile advertising systems though lack reliable browser tracking while
9 traditional online advertising relies on the use of browser cookies.

10 Implementations inherent in conventional mobile ad serving have effectively
11 prevented mobile advertising from being effective because of its inability to
12 obtain mobile device "uniqueness." In order to obtain such uniqueness, the
13 mobile advertising industry sought a means to obtain unique device identifiers
14 which provide a unique reference to individual mobile devices. Unlike traditional
15 cookies, such identifiers are hard coded into a user's phones software, and thus a
16 user has no ability to disable mobile device identifiers.

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

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

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

12 Patent No.: US 7,609,650 B2

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

14 Filed: July 5, 2005

15 Inventor: Konstantin Othmer

16 51. The dilemma facing the mobile advertising industry is that once the
17 mobile device data was extracted a system and method was needed to for
18 wireless devices to use data for mobile advertising. Provided such a mechanism.
19 While Carrier IQ may have concentrated on extraction of mobile device metrics,
20 other companies were interested in assisting the mobile advertising networks to
21 use mobile device data.

22 **C. IQ Agent Technology**

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

25 52. Plaintiffs' independent investigation of the IQ Agent software
26 revealed a number of interesting factors not found in any study or account by
27 Samsung or Carrier IQ:

28 53. 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 Samsung IQ Agent prompts the operating system to append an entry into the log file.

54. 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.

55. 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*

56. 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.

57. 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*

58. 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.

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

4 60. A user is unable to stop the Carrier IQ software from running. When
5 a user manually turns off the IQ Agent software, it automatically restarts itself
6 seconds later. A user is unable to delete or remove the IQ Agent software from
7 the device without voiding Samsung's manufacturer's warranty.

8 61. Because the software is preinstalled by Samsung and runs as part of
9 the device operating system, data is continuously collected and can be transmitted
10 via wireless internet or other means, even if the device user has no carrier
11 contract and the mobile device is not connected to a mobile network.

12 iv. *IQ Agent Depletion of Resources*

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

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

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

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

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

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

1 **D. Samsung's Warranty**

2 63. There is no choice to "opt in" to Carrier IQ's data collection and
3 transmission by downloading IQ Agent since in many cases it is preinstalled or
4 installed via automatic update on Plaintiffs' and Class Members' mobile devices.
5 Users cannot uninstall it, block it, or cease its actions. Samsung and Carrier IQ
6 provide Plaintiffs and Class Members no notice of this software or the functions
7 it performs.

8 64. Samsung's Manufacturer's Warranty for the Samsung mobile
9 devices does not mention or disclose the existence of the IQ Agent software on
10 the device or the functions that software performs.

11 65. Samsung's Manufacturer's Warranty states that the Warranty will be
12 void if a user alters the operating system or opens or tampers with the device's
13 software, which would include deleting or attempting to delete the IQ Agent
14 software from the device.

15 **E. Defendants' Harmful Business Practices**

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

24 67. Defendants' collection and disclosure of this personal information
25 violates user expectations, diminished user's privacy, and contradicted the
26 Samsung's own representations. These business practices are unfair and
27 deceptive trade practices as set forth further below.

28 68. Defendants harmed Plaintiffs and Class Members when they

1 purchased the Samsung device IQ Agent. In selecting the Samsung mobile device
2 over the service and goods of other competing mobile phone manufacturers,
3 Plaintiffs and Class Members reasonably expected that their confidential user
4 data would not be accessed and transmitted to third parties without their
5 knowledge and consent.

6 69. Defendants harmed Plaintiff and Class Members by obtaining their
7 confidential user data and device resources.

8 70. Carrier IQ exercises substantial control over its development and
9 functionality on Samsung's mobile devices. Carrier IQ and Samsung must agree
10 to the terms of Carrier IQ's License Agreement in order to have Carrier IQ
11 function on Samsung mobile device. Carrier IQ will only function on mobile
12 devices by interacting with a mobile device's operating system and features in the
13 ways permitted by such an agreement.

14 71. Carrier IQ's control of the user experience includes restrictions, such
15 as blocking consumers from modifying its software. As a direct consequence of
16 the control exercised by Carrier IQ, Plaintiffs and the Class cannot reasonably
17 review the privacy effects of IQ Agent.

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

27 73. Defendants' activities made the basis of this action consume vast
28 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.

74. Plaintiffs and Class Members were afforded only a millisecond of time after activating their Samsung mobile device before IQ Agent intentionally, and without users' authorization and consent, accessed Plaintiffs' 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

75. Plaintiffs bring 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 Samsung mobile device on which the IQ Agent software resides from December 4, 2007 to December 4, 2011.

76. Plaintiffs 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 Samsung mobile device on which the IQ Agent software resides from December 4, 2007 to December 4, 2011.

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

78. This action is brought as a class action and may properly be so

1 maintained pursuant to the provisions of Federal Rule of Civil Procedure 23.
2 Plaintiffs reserve the right to modify the Nationwide Class and the Texas
3 Subclass definitions and the class period pursuant to discovery that is conducted
4 hereafter.

5 79. The members of the Class are so numerous that joinder of all
6 members would be impracticable. Plaintiffs estimate that there are hundreds of
7 thousands of consumers who purchased Samsung mobile devices installed with
8 the IQ Agent software.

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

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

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

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

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

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

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

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

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

7 (i) whether Defendants' conduct constitutes trespass; and

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

11 81. Plaintiffs' claims are typical of the claims of the members of the
12 Class. Plaintiffs have no interests antagonistic to those of the Class and are
13 subject to no unique defenses.

14 82. Plaintiffs will fairly and adequately protect the interests of the Class
15 and have retained attorneys experienced in class and complex litigation.

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

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

20 (b) The Class is readily definable;

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

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

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

27 (f) Plaintiffs do not anticipate any difficulty in the management
28 of this litigation as a class action.

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

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

7 **VIII. CAUSES OF ACTION**

8 **FIRST CAUSE OF ACTION**

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

10 **Against All Defendants**

11 86. Plaintiffs incorporate by reference all paragraphs previously alleged
12 herein.

13 87. Plaintiffs assert this claim against each and every Defendant named
14 herein in this complaint on behalf of themselves and the Class.

15 88. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §
16 2510, referred to as "ECPA," regulates wire and electronic communications
17 interception and interception of oral communications, and makes it unlawful for a
18 person to "willfully intercept, endeavor to intercept, or procure any other person
19 to intercept or endeavor to intercept, any wire, oral, or electronic
20 communication," within the meaning of 18 U.S.C. § 2511(1).

21 89. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring
22 and/or intercepting, by device or otherwise, Plaintiffs' and Class Members'
23 electronic communications, without knowledge, consent, or authorization.

24 90. At all relevant times, Defendants engaged in business practices of
25 intercepting and collecting the Plaintiffs' and Class Members' confidential
26 electronic communications which included incoming text messages, URLs of
27 websites viewed and GPS coordinates from within their mobile devices. Once
28 Defendants obtained this confidential personal information, Defendants used it to

1 aggregate mobile device data regarding Plaintiffs' and Class Members' uses of
2 their mobile devices. Defendants also made this confidential and unencrypted
3 data available to any device software or application with log file access, further
4 violating Plaintiffs' and Class Members' privacy.

5 91. The contents of data transmissions from and to Plaintiffs' and Class
6 Members' personal computers constitute "electronic communications" within the
7 meaning of 18 U.S.C. §2510.

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

11 93. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally
12 intercepting, endeavoring to intercept, or procuring any other person to intercept
13 or endeavor to intercept Plaintiffs' and Class Members' electronic
14 communications.

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

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

25 96. Defendants' intentional interception of these electronic
26 communications without Plaintiffs' or Class Members' knowledge, consent, or
27 authorization was undertaken without a facially valid court order or certification.

28 97. Defendants intentionally used such electronic communications, with

1 knowledge, or having reason to know, that the electronic communications were
2 obtained through interception, for an unlawful purpose.

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

8 99. The Electronic Communications Privacy Act of 1986, 18 USC
9 §2520(a) provides a civil cause of action to "any person whose wire, oral, or
10 electronic communication is intercepted, disclosed, or intentionally used" in
11 violation of the ECPA.

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

18 101. Plaintiffs and Class Members have additionally suffered loss by
19 reason of these violations, including, without limitation, violation of the right of
20 privacy. Defendants exposed Plaintiffs' and Class Members' personal
21 information to any third party software or application with log file access residing
22 on their mobile devices without Plaintiffs' or Class Members' permission or
23 knowledge, and in an unencrypted format. Plaintiffs and Class Members were
24 damaged by Defendants' unauthorized use of the resources of Plaintiff's and
25 Class Members' mobile devices including battery power, device memory, CPUs,
26 and bandwidth. Plaintiffs and Class Members had unauthorized charges to their
27 mobile devices for every hidden text message that was sent by Defendants.

28 102. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to

1 preliminary, equitable, and declaratory relief, in addition to statutory damages of
2 the greater of \$10,000 or \$100 a day for each day of violation, actual and punitive
3 damages, reasonable attorneys' fees, and Defendants' profits obtained from the
4 above-described violations. Unless restrained and enjoined, Defendants will
5 continue to commit such acts. Plaintiffs' and Class Members' remedy at law is
6 not adequate to compensate it for these inflicted and threatened injuries, entitling
7 Plaintiffs and Class Members to remedies including injunctive relief as provided
8 by 18 U.S.C. § 2510.

9 **SECOND CAUSE OF ACTION**

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

11 **Against All Defendants**

12 103. Plaintiffs incorporate the above allegations by reference as though
13 fully set forth herein.

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

17 105. Defendants were engaged in the sale of mobile devices to consumers
18 during the class period.

19 106. Defendants intentionally accessed and collected the personal data of
20 Plaintiffs and Class Members on their mobile devices without notice or
21 authorization, including incoming text messages, URLs of websites viewed and
22 GPS coordinates.

23 107. As a result of Defendants' unlawful violation of this section,
24 Plaintiffs and Class Members have been damaged by among other things, failing
25 to receive the benefits of a product impliedly represented to them as secure as to
26 their personal information. Plaintiffs and Class Members have additionally
27 suffered loss by reason of these violations, including violation of their rights of
28 privacy. Defendants exposed Plaintiffs' and Class Members' personal

1 information to any third party software or application with log file access residing
2 on their mobile devices without Plaintiffs' or Class Members' permission or
3 knowledge, and in an unencrypted form. Plaintiffs and Class Members were
4 damaged by Defendants' unauthorized use of the resources of Plaintiffs' and
5 Class Members' mobile devices including battery power, cell phone memory,
6 CPUs, and bandwidth. Moreover, Plaintiffs and Class Members had unauthorized
7 charges to their mobile devices for every hidden text message that was sent by
8 Defendants.

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

14 **THIRD CAUSE OF ACTION**

15 **Violation of the Consumer Legal Remedies Act**

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

17 **Against All Defendants**

18 109. Plaintiffs incorporate the foregoing allegations as if fully set forth
19 herein.

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

27 111. At all relevant times, Defendants' business practices of selling
28 Samsung mobile devices installed or updated with IQ Agent software, were

1 goods Plaintiffs and Class Members obtained for use. Defendants' scheme to
2 offer such goods misled Plaintiffs and Class Members about the nature and
3 integrity of the Samsung mobile devices since Defendants intended to use such
4 for mobile device tracking, collection of confidential, unencrypted user data, and
5 depletion of consumer resources, including battery power, device memory,
6 CPUs, and bandwidth. Defendants also charged consumers for every hidden text
7 message that was sent by Defendants.

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

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

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

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

11 116. Plaintiffs, on behalf of themselves and on behalf of each member of
12 the Class, shall seek individual restitution, injunctive relief, and other relief as the
13 Court deems just and proper.

14 117. Pursuant to California Civil Code, Section 1782, Plaintiffs will
15 notify Defendants in writing of the particular violations of Civil Code, Section
16 1770 and demand that Defendants rectify the problems associated with its
17 behavior detailed above, which acts and practices are in violation of Civil Code
18 Section 1770.

19 **FOURTH CAUSE OF ACTION**

20 **Violation of Unfair Competition California Business and Professions Code §** 21 **17200**

22 **Against All Defendants**

23 118. Plaintiffs incorporate the foregoing allegations as if fully set forth
24 herein.

25 119. In violation of California Business and Professions Code Section
26 17200 et seq., Defendants' conduct in this regard is ongoing and includes, but is
27 not limited to, unfair, unlawful and fraudulent conduct.

28 120. At all relevant times, Defendants' business practices as alleged

1 above constitute unlawful, unfair and fraudulent business acts and practices.

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

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

11 **A. Unlawful Business Act and Practices**

12 123. Defendants' business acts and practices are unlawful, in part,
13 because they violate the Electronic Communications Privacy Act, 18 U.S.C.
14 Section 2510 which prohibits any person from willfully intercepting or
15 endeavoring to intercept, or procuring any other person to intercept or endeavor
16 to intercept, any wire, oral, or electronic communication, including incoming text
17 messages.

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

22 **B. Unfair Business Act and Practices**

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

27 126. Defendants' conduct lacks reasonable and legitimate justification in
28 that Defendants have benefited from such conduct and practices while Plaintiffs

1 and the Class Members have been misled as to the nature and integrity of
2 Defendants' services and have, in fact, suffered injury regarding the privacy and
3 confidentiality of their personal information and the use of their device resources.
4 Defendants' conduct offends public policy in California in connection with the
5 Consumer Legal Remedies Act, the state constitutional right of privacy, and
6 California statutes recognizing the need for consumers to safeguard their own
7 privacy interests, including California Civil Code, Section 1798.80.

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

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

16 129. Defendants' practice of capturing, storing, and transferring highly
17 detailed and personal records of consumers' incoming text messages, URLs of
18 websites visited and GPS location histories, and storing such information in
19 unencrypted form, is in violation of the Unfair Competition Law. Plaintiffs and
20 Class Members have suffered loss by reason of these violations, including,
21 violation to their right of privacy. Defendants exposed Plaintiffs' and Class
22 Members' personal information to any third party software or applications with
23 log file access residing on their mobile devices without Plaintiffs' or Class
24 Members' consent or knowledge, and in an unencrypted form. Plaintiffs and
25 Class Members were damaged by Defendants' unauthorized use of the resources
26 of Plaintiff's and Class Members' mobile devices including battery power, cell
27 phone memory, CPUs, and bandwidth. Moreover, Plaintiffs and Class Members
28 had to pay unauthorized charges to their mobile devices for every hidden text

1 message that was sent by Defendants.

2 **FIFTH CAUSE OF ACTION**

3 **Violation of California's Computer Crime Law**

4 **Penal Code § 502 et seq.**

5 **Against All Defendants**

6 130. Plaintiffs incorporate the above allegations by reference as if set
7 forth herein at length.

8 131. The California Computer Crime Law, California Penal Code Section
9 502 regulates "tampering, interference, damage, and unauthorized access to
10 lawfully created computer data and computer systems." A mobile device is a
11 "computer system" as defined in Penal Code Section 502(b)(5) in that it contains
12 electronic instructions, inputs and outputs data, performs functions including
13 communication and data storage and retrieval.

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

20 133. At all relevant times, Defendants had a business practice of
21 accessing Plaintiffs' and Class Members' mobile devices on a systematic and
22 continuous basis in order to obtain mobile device data and to monitor and collect
23 data related to their browsing habits, GPS locations and incoming text messages.
24 Defendants accessed such data without notice to or authorization from Plaintiffs
25 or Class Members.

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

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

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

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

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

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

22 140. Defendants have violated California Penal Code § 502(c)(6) by
23 knowingly and without permission providing, or assisting in providing, a means
24 of accessing Plaintiffs' mobile device and mobile device system.

25 141. Defendants has violated California Penal Code § 502(c)(7) by
26 knowingly and without permission accessing, or causing to be accessed,
27 Plaintiffs' mobile device and mobile device system.

28 142. California Penal Code § 502(j) states: "For purposes of bringing a

1 civil or a criminal action under this section, a person who causes, by any means,
2 the access of a computer, computer system, or computer network in one
3 jurisdiction from another jurisdiction is deemed to have personally accessed the
4 computer, computer system, or computer network in each jurisdiction.”

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

15 144. Plaintiffs have also suffered irreparable injury from these
16 unauthorized acts of disclosure, to wit: their personal, private, and sensitive
17 electronic data was obtained and used by Defendant. Due to the continuing threat
18 of such injury, Plaintiffs have no adequate remedy at law, entitling Plaintiffs to
19 injunctive relief.

20 145. Plaintiffs and Class Members have additionally suffered loss by
21 reason of these violations, including, without limitation, violation of the right of
22 privacy and depletion of valuable device resources.

23 146. As a direct and proximate result of Defendants’ unlawful conduct
24 within the meaning of California Penal Code § 502, Defendants have caused loss
25 to Plaintiffs in an amount to be proven at trial. Plaintiffs are also entitled to
26 recover their reasonable attorneys’ fees pursuant to California Penal Code §
27 502(e).

28 147. Plaintiffs and the Class Members seek compensatory damages, in an

1 amount to be proven at trial, and injunctive or other equitable relief.

2 **SIXTH CAUSE OF ACTION**

3 **Violation of the California Invasion of Privacy Act**

4 **Penal Code § 630 et seq.**

5 **Against All Defendants**

6 148. Plaintiffs incorporate the above allegations by reference as if set
7 forth herein at length.

8 149. California Penal Code Section 630 provides, in part:

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

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

1 Plaintiff or Class Members.

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

7 152. Communications from the California web-based entities to Plaintiffs
8 and Class Members were sent from California. Communications to the California
9 web-based entities from Plaintiffs and Class Members were sent to California.

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

13 154. Plaintiffs and Class Members did not consent to any of the
14 Defendants' actions in using the contents of their communications with such
15 California-based entities.

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

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

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

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

27 159. Defendants directly participated in intercepting, reading, and/or
28 learning the contents of the communications between Plaintiffs, Class Members

1 and California-based web entities.

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

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

16 162. Unless restrained and enjoined, Defendants will continue to commit
17 such acts. Pursuant to § 637.2 of the California Penal Code, Plaintiffs and the
18 Class have been injured by the violations of California Penal Code Section 631.
19 Wherefore, Plaintiffs, on behalf of themselves and on behalf of a similarly
20 situated Class of consumers, seek damages and injunctive relief.

21 **SEVENTH CAUSE OF ACTION**

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

23 **Against All Defendants**

24 163. Plaintiffs hereby incorporate by reference the allegations contained
25 in all the paragraphs of this Complaint.

26 164. Samsung warranted to Plaintiffs and Class Members in its
27 "Manufacturer's Warranty" that the mobile devices would be free from defects
28 for normal consumer usage for twelve months from the date of purchase.

1 165. Samsung by offering mobile devices in the marketplace represented
2 and warranted to Plaintiffs and Class Members that these devices did not cause
3 personal information to be unreasonably and unexpectedly transferred to third
4 parties.

5 166. Plaintiffs and Class Members paid more for their mobile devices
6 than they would have paid if Samsung disclosed the fact that the mobile devices
7 were designed with defects, namely the privacy breach to Carrier IQ and any
8 other third party software on the mobile device.

9 167. A reasonable consumer would, and Plaintiffs and Class Members
10 did expect that, if Samsung mobile devices were subject to defects such as those
11 identified above, Samsung would disclose these material facts and Plaintiffs and
12 Class Members would not have purchased these devices.

13 168. Plaintiffs and Class Members paid premiums for Samsung mobile
14 devices because they reasonably believed the devices were designed to employ
15 reasonable security in their operation.

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

19 170. Moreover, Samsung asserts that disabling the Carrier IQ software on
20 a mobile device voids the Samsung Warranty. Plaintiffs and Class Members are
21 therefore forced to induce breach of the Samsung Warranty by disabling the
22 Carrier IQ software to protect their personal information.

23 171. Plaintiffs and Class Members who purchased the mobile devices are
24 entitled to a refund of the purchase price.

25 **EIGHTH CAUSE OF ACTION**

26 **Texas Deceptive Trade Practices Act, Business and Commerce**

27 **Code § 17.41 et seq.**

28 **Against All Defendants**

CLASS ACTION COMPLAINT

1 172. Plaintiffs hereby incorporate by reference the allegations contained
2 in all of the preceding paragraphs of this complaint.

3 173. Plaintiffs are “consumers” under the Texas Deceptive Trade
4 Practices Act as they purchased and used Samsung mobile devices that had been
5 preinstalled with the Carrier IQ tracking program.

6 174. Defendants are proper “persons” or defendants under the Texas
7 Deceptive Trade Practices Act, who either used or employed false, misleading,
8 deceptive or unconscionable acts or practices, or were directly connected with the
9 transaction with Plaintiffs.

10 175. Defendants committed multiple violations and wrongful acts under
11 the Texas Deceptive Trade Practices Act, including the following: making or
12 committing, false, misleading or deceptive acts and/or practices, including but
13 not limited to violations of Tex. Business & Commerce Code § 17.46(b) (3), (5),
14 (7), (9), (20), and (24). Defendants committed misleading and unconscionable
15 acts in connection with the sale of mobile devices installed or updated with IQ
16 Agent to Plaintiffs and Class Members, and the subsequent tracking and logging
17 of Plaintiffs’ and Class Members’ confidential, unencrypted through IQ Agent
18 without notice or consent. In carrying out these acts, Defendants depleted
19 Plaintiffs’ and Class Members’ mobile device resources without notice to or
20 consent from Plaintiffs or Class Members. Plaintiffs and Class Members relied on
21 Defendants’ acts and/or practices to their detriment.

22 176. Plaintiffs will show that the violation and actions of Defendants
23 were a producing cause of their damages. Defendants exposed Plaintiffs’ and
24 Class Members’ personal information to any third party software or applications
25 with log file access residing on their mobile devices without Plaintiffs’ or Class
26 Members’ permission or knowledge, and in an unencrypted form. Plaintiffs and
27 Class Members were damaged by Defendants’ unauthorized use of Plaintiffs’ and
28 Class Members’ mobile device resources including battery power, cell phone

1 memory, CPUs, and bandwidth. Moreover, Plaintiffs and Class Members had
2 unauthorized charges to their mobile devices for every hidden text message that
3 was sent by Defendants.

4 177. Plaintiffs will show that the violations and actions of Defendants
5 were done intentionally or knowingly, entitling Plaintiffs to treble damages.

6 178. Plaintiffs will show that the violations and actions of Defendants
7 entitle them to reasonable and necessary attorney's fees under the Texas
8 Deceptive Trade Practices Act, specifically Tex. Business & Commerce Code §
9 17.50(d).

10 **NINTHCAUSE OF ACTION**

11 **Breach of Express Warranty**

12 **Against Defendant Samsung**

13 179. Plaintiffs hereby incorporate by reference the allegations contained
14 in all the paragraphs of this Complaint.

15 180. Samsung warranted to Plaintiffs and Class Members in its
16 "Manufacturer's Warranty" that the mobile devices would be free from defects
17 for normal consumer usage for twelve months from the date of purchase.

18 181. Samsung by sold mobile devices to Plaintiffs and Class Members
19 that were defective because they caused personal information to be unreasonably
20 and unexpectedly viewed and collected by Carrier IQ and other third party
21 software and applications. The devices also were subject to depletion of resources
22 through the IQ Agent software which depleted those resources without notice to
23 or authorization from Plaintiffs or Class Members.

24 182. Plaintiffs and Class Members paid more for their mobile devices
25 than they would have paid if Samsung disclosed the fact that the mobile devices
26 were designed with defects, namely the privacy breach and depletion of mobile
27 device resources.

28 183. A reasonable consumer would, and Plaintiffs and Class Members

1 did expect that, if Samsung mobile devices were subject to defects such as those
2 identified above, Samsung would disclose these material facts and Plaintiffs and
3 Class Members would not have purchased these devices.

4 184. Plaintiffs and Class Members paid premiums for Samsung mobile
5 devices because they reasonably believed the devices were designed to employ
6 reasonable security in their operation.

7 185. Samsung's failure to provide to Plaintiffs and Class Members a
8 mobile device that is not defective is a violation of Samsung's express warranty.

9 186. Moreover, Samsung asserts that disabling the Carrier IQ software on
10 a mobile device voids the Samsung warranty. Plaintiffs and Class Members are
11 therefore forced by Samsung to induce breach of the Samsung Warranty by
12 disabling the Carrier IQ software to protect their personal information.

13 187. Plaintiffs and Class Members who purchased the mobile devices are
14 entitled to a refund of the purchase price.

15 **TENTH CAUSE OF ACTION**

16 **Breach of Implied Warranty**

17 **Against Defendant Samsung**

18 188. Plaintiffs hereby incorporate by reference the allegations contained
19 in all the paragraphs of this Complaint.

20 189. Samsung by offering mobile devices in the marketplace represented
21 and warranted to Plaintiffs and Class Members that these devices would be free
22 from defects for normal consumer usage and would not cause personal
23 information to be unreasonably and unexpectedly transferred to third parties.

24 190. Samsung by sold mobile devices to Plaintiffs and Class Members
25 that were defective because they caused personal information to be unreasonably
26 and unexpectedly viewed and collected by Carrier IQ and other third party
27 software and applications. The devices also were subject to depletion of resources
28 through the IQ Agent software which depleted those resources without notice to

1 or authorization from Plaintiffs or Class Members.

2 191. Plaintiffs and Class Members paid more for their mobile devices
3 than they would have paid if Samsung disclosed the fact that the mobile devices
4 were designed with defects, namely the privacy breach and depletion of mobile
5 device resources..

6 192. A reasonable consumer would, and Plaintiffs and Class Members
7 did expect that, if Samsung mobile devices were subject to defects such as those
8 identified above, Samsung would disclose these material facts and Plaintiffs and
9 Class Members would not have purchased these devices.

10 193. Plaintiffs and Class Members paid premiums for Samsung mobile
11 devices because they reasonably believed the devices were designed to employ
12 reasonable security in their operation.

13 194. Samsung's failure to provide to Plaintiffs and Class Members a
14 mobile device that is not defective is a violation of Samsung's implied warranty.

15 195. Plaintiffs and Class Members who purchased the mobile devices are
16 entitled to a refund of the purchase price.

17 **ELEVENTH CAUSE OF ACTION**

18 **Negligence**

19 **Against All Defendants**

20 196. Plaintiffs incorporate the above allegations by reference as if fully
21 set forth herein.

22 197. Carrier IQ and Samsung owed a duty of care to Plaintiffs and Class
23 Members.

24 198. Carrier IQ and Samsung breached their duty by negligently
25 designing IQ Agent and preinstalling or uploading it to Plaintiffs' and Class
26 Members' mobile devices without any notice or authorization so that Defendants
27 could acquire personal information without Plaintiffs' and Class Members'
28 knowledge or permission. Defendants also negligently made this confidential

1 data available to any software or application with log file access on the mobile
2 device, in an unencrypted format. Defendants also negligently depleted Plaintiffs'
3 and Class Members' mobile device resources.

4 199. Carrier IQ and Samsung failed to fulfill their own commitments to
5 Plaintiffs and Class Members, and further failed to fulfill even the minimum duty
6 of care to protect Plaintiffs' and Class Members' personal information, privacy
7 rights, security, and device resources.

8 200. Samsung's unencrypted storage of Plaintiffs' and Class Members'
9 on the mobile device log file and Carrier IQ servers was negligent.

10 201. Plaintiffs and Class Members were harmed as a result of Carrier
11 IQ's breaches of its duty, and Carrier IQ proximately caused such harms.

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

19 203. Samsung's preinstallation or upload of IQ Agent and unauthorized
20 use of Plaintiffs' and Class Members' confidential information without notice to
21 or consent from Plaintiffs or Class Members was negligent.

22 204. Defendants exposed Plaintiffs' and Class Members' personal
23 information to any third party software with log file access residing on their
24 mobile devices without Plaintiffs' or Class Members' permission or knowledge,
25 and in an unencrypted form. Plaintiffs and Class Members were damaged by
26 Defendants' unauthorized use of the resources of their mobile devices including
27 battery power, cell phone memory, CPUs, and bandwidth. Moreover, Plaintiffs
28 and Class Members had unauthorized charges to their mobile devices for every

1 hidden text message that was sent by Carrier IQ.

2 205. Plaintiffs and Class Members were harmed as a result of
3 Defendants' breaches of their duty, and Defendants proximately caused such
4 harms.

5 **TWELFTH CAUSE OF ACTION**
6 **Trespass to Personal Property/Chattels**
7 **Against All Defendants**

8 206. Plaintiffs incorporate by reference all paragraphs previously alleged
9 herein.

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

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

22 209. Without Plaintiffs' and Class Members' consent, or in excess of any
23 consent given, Defendants knowingly and intentionally accessed Plaintiffs' and
24 Class Members' property, thereby intermeddling with Plaintiffs' and Class
25 Members' right to possession of the property and causing injury to Plaintiffs and
26 the members of the Class.

27 210. Defendants engaged in deception and concealment in order to gain
28 access to Plaintiffs' and Class Members' mobile devices.

1 211. Defendants undertook the following actions with respect to
2 Plaintiffs' and Class Members' mobile devices:

3 212. Defendants accessed and obtained control over the users' mobile
4 device;

5 213. Defendants caused the installation of code on the hard drives of the
6 mobile devices;

7 214. Defendants programmed the operation of its code to circumvent the
8 mobile device owners' privacy and security controls, to remain beyond their
9 control, and to continue to function and operate without notice to them or consent
10 from Plaintiffs and Class Members;

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

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

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

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

24 219. Defendants' installation and operation of its program used,
25 interfered, and/or intermeddled with Plaintiffs' and Class Members' mobile
26 devices. Such use, interference and/or intermeddling was without Plaintiffs' and
27 Class Members' consent or, in the alternative, in excess of Plaintiffs' and Class
28 Members' consent.

1 220. Defendants' installation and operation of its program constitutes
2 trespass, nuisance, and an interference with Plaintiffs' and Class Members'
3 chattels, to wit, their mobile devices.

4 221. Defendants' installation and operation of the Carrier IQ program
5 impaired the condition and value of Plaintiffs' and Class Members' mobile
6 devices.

7 222. Defendants' trespass to chattels, nuisance, and interference caused
8 real and substantial damage to Plaintiffs and Class Members. Defendants exposed
9 Plaintiffs' and Class Members' personal information to any third party software
10 with log file access residing on their mobile devices without Plaintiffs' or Class
11 Members' permission or knowledge, and in an unencrypted form. Plaintiffs and
12 Class Members were damaged by Defendants' unauthorized use of the resources
13 of Plaintiff's and Class Members' mobile devices including battery power, cell
14 phone memory, CPUs, and bandwidth. Plaintiffs and Class Members had
15 unauthorized charges to their mobile devices for every hidden text message that
16 was sent by Carrier IQ.

17 223. As a direct and proximate result of Defendants' trespass to chattels,
18 nuisance, interference, unauthorized access of and intermeddling with Plaintiffs'
19 and Class Members' property, Defendants have injured and impaired Plaintiffs
20 and Class Members in the condition and value of Plaintiffs' Class Members'
21 mobile devices, as follows:

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

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

28 (c) By devaluing, interfering with, and/or diminishing

1 Plaintiffs' and Class Members' possessory interest in their mobile devices;

2 (d) By altering and/or controlling the functioning of Plaintiffs'
3 and Class Members' mobile devices;

4 (e) By infringing on Plaintiffs' and Class Members' right to
5 exclude others from their mobile devices;

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

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

11 (h) By utilizing Plaintiffs' and Class Members' mobile device
12 resources without notice or consent.

13 **THIRTEENTH CAUSE OF ACTION**

14 **Unjust Enrichment**

15 **Against All Defendants**

16 224. Plaintiffs hereby incorporate by reference the allegations contained
17 in all of the paragraphs of this complaint.

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

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

27 227. Defendants appreciate and/or have knowledge of said benefit.

28 228. Under principles of equity and good conscience, Defendants should

1 not be permitted to retain the information and/or revenue that they acquired by
2 virtue of their unlawful conduct. All funds, revenue, and benefits received by
3 them rightfully belong to Plaintiffs and the Class, which the Defendants have
4 unjustly received as a result of their actions.

5 229. Plaintiffs and Class Members have no adequate remedy at law.

6 230. Defendants have received a benefit from Plaintiffs and Class
7 Members and Defendants have received and retained money or other benefits
8 from third parties as a result of sharing Plaintiffs' and Class Members'
9 confidential information of Plaintiffs and Class Members without Plaintiffs' or
10 Class Members' knowledge or consent as alleged in this Complaint.

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

14 232. Defendants knowingly used Plaintiffs' and Class Members'
15 confidential information without their knowledge or consent to gain commercial
16 advantage from third parties and had full knowledge of the benefits they have
17 received from Plaintiffs and Class Members. If Plaintiffs and Class Members had
18 known Defendants were not keeping their confidential information from third-
19 parties, they would not have consented and Defendants would not have gained
20 commercial or business advantage from third parties.

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

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

27 235. Plaintiffs and the Members of the Class are entitled to an award of
28 compensatory and punitive damages in an amount to be determined at trial or to

1 be imposition of a constructive trust upon the wrongful revenues and/or profits
2 obtained by and benefits conferred upon Defendants as a result of the wrongful
3 actions as alleged in this complaint.

4 236. Plaintiffs and the Class have no remedy at law to prevent Defendants
5 from continuing the inequitable conduct alleged in this complaint and the
6 continued unjust retention of the money and/or benefits Defendants received
7 from third parties.

8 **FOURTEENTH CAUSE OF ACTION**

9 **Conversion**

10 **Against All Defendants**

11 237. Plaintiffs hereby incorporate by reference the allegations contained
12 in all of the preceding paragraphs of this complaint.

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

20 239. Plaintiffs' and Class Members' mobile devices use battery power,
21 cell phone memory, CPUs, and bandwidth. Defendants' activities, made the basis
22 of this action, used without notice or authorization, such battery power, memory,
23 CPU and bandwidth for purposes not contemplated and not agreed to by
24 Plaintiffs and Class Members when they purchased their Samsung mobile
25 devices. Such property, owned by Plaintiffs and Class Members, is valuable to
26 Plaintiffs and Class Members. Plaintiffs and Class Members were damaged by
27 Defendants' unauthorized use of Plaintiff's and Class Members' battery power,
28 cell phone memory and CPUs, as well as bandwidth. Moreover, Defendants

1 utilized Plaintiffs' and Class Members' limited text messages in order to send
2 secret and unauthorized instructions to their mobile devices. Plaintiffs and Class
3 Members paid unauthorized charges for every hidden text message that was sent
4 by Defendants.

5 240. Defendants unlawfully exercised dominion over said property and
6 thereby converted Plaintiffs' and Class Members' property.

7 241. Plaintiffs and Class Members were damaged by Defendants' actions.

8 **PRAYER FOR RELIEF**

9 WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly
10 situated, pray for judgment against Defendants as follows:

11 A. Certify this case as a Class action on behalf of the Classes defined
12 above, appoint Plaintiffs as Class representatives, and appoint their counsel as
13 Class counsel;

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

16 C. Award injunctive and equitable relief including, *inter alia*: (i)
17 prohibiting Defendants from engaging in the acts alleged above; (ii) requiring
18 Defendants to disgorge all of their ill-gotten gains to Plaintiffs and Class
19 Members, or to whomever the Court deems appropriate; (iii) requiring
20 Defendants to delete all data surreptitiously or otherwise collected data through
21 the acts alleged above; (iv) requiring Defendants to provide Plaintiffs and Class
22 Members a means to easily and permanently decline any participation in any data
23 collection activities; (v) awarding Plaintiffs and Class Members full restitution of
24 all benefits wrongfully acquired by Defendants by means of the wrongful
25 conduct alleged herein; and (vi) ordering an accounting and constructive trust
26 imposed on the data, funds, or other assets obtained by unlawful means as alleged
27 above, to avoid dissipation, fraudulent transfers, and/or concealment of such
28 assets by Defendants;

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

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

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

9 G. Award Plaintiffs and the Classes:

10 (i) Compensatory damages sustained by Plaintiffs and
11 all others similarly situated as a result of Defendants' unlawful acts and
12 conduct;

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

15 (k) Plaintiffs' reasonable litigation expenses and
16 attorneys' fees;

17 (l) Pre- and post-judgment interest, to the extent
18 allowable;

19 (m) Statutory damages, including punitive damages; and

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

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

23 Dated this 8th day of December, 2011.

24
25 By: 

26 STRANGE & CARPENTER

27 Brian R. Strange (Cal. Bar. No. 103252)
28 LACounsel@earthlink.net
12100 Wilshire Boulevard, Suite 1900

1 Los Angeles, CA 90025
2 Telephone: (310) 207-5055
3 Facsimile: (310) 826-3210

4 Law Office of Joseph H. Malley
5 Joseph H. Malley (not admitted)
6 malleylaw@gmail.com
7 1045 North Zang Blvd
8 Dallas, TX 75208
9 Telephone: (214) 943-6100

10 *Counsel for Plaintiffs and the Proposed*
11 *Class*

1
2 **JURY TRIAL DEMAND**

3 The Plaintiffs hereby demand a trial by jury of all issues so triable.

4 Dated this 8th day of December, 2011.
5

6 
7 _____
8 By:

9 STRANGE & CARPENTER

10 Brian R. Strange (Cal. Bar. No. 103252)
11 LACounsel@earthlink.net
12 12100 Wilshire Boulevard, Suite 1900
13 Los Angeles, CA 90025
14 Telephone: (310) 207-5055
15 Facsimile: (310) 826-3210

16 Law Office of Joseph H. Malley
17 Joseph H. Malley (not admitted)
18 malleylaw@gmail.com
19 1045 North Zang Blvd
20 Dallas, TX 75208
21 Telephone: (214) 943-6100

22 *Counsel for Plaintiffs and the Proposed*
23 *Class*
24
25
26
27
28

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge Andrew Guilford and the assigned discovery Magistrate Judge is Jean P. Rosenbluth.

The case number on all documents filed with the Court should read as follows:

SACV11- 1899 AG (JPRx)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

=====

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

☐ **Western Division**
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

☒ **Southern Division**
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

☐ **Eastern Division**
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.

Brian R. Strange, 103252
STRANGE & CARPENTER
12100 Wilshire Blvd., Suite 1900
Los Angeles, California 90025
Tel: (310) 207-5055

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

LISA CLARK, FELIPE GARCIA and ROBERT
SPRADLEY; individuals, on behalf of themselves and
others similarly situated,

PLAINTIFF(S)

v.

CARRIER IQ, INC., a Delaware Corporation;
SAMSUNG ELECTRONICS AMERICA, INC., and
SAMSUNG TELECOMMUNICATIONS AMERICA,
LLC

DEFENDANT(S).

CASE NUMBER

SACV11-01899 AG (JPRx)

SUMMONS

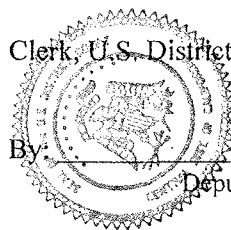
TO: DEFENDANT(S): Carrier IQ, Inc., a Delaware Corporation; Samsung Electronics America, Inc.,
and Samsung Telecommunications America, LLC

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it), you must serve on the plaintiff an answer to the attached ☒ complaint ☐ amended complaint ☐ counterclaim ☐ cross-claim or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff's attorney, Brian R. Strange, whose address is 12100 Wilshire Blvd., Suite 1900, Los Angeles, California 90025. If you fail to do so, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Dated: 8 2011

Clerk, U.S. District Court



AMY DeAVILA

Deputy Clerk

(Seal of the Court)

[Use 60 days if the defendant is the United States or a United States agency, or is an officer or employee of the United States. Allowed 60 days by Rule 12(a)(3)].

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET**

I (a) PLAINTIFFS (Check box if you are representing yourself <input type="checkbox"/>) LISA CLARK, FELIPE GARCIA and ROBERT SPRADLEY; individuals, on behalf of themselves and others similarly situated	DEFENDANTS CARRIER IQ, INC., a Delaware Corporation; SAMSUNG ELECTRONICS AMERICA, INC., and SAMSUNG TELECOMMUNICATIONS AMERICA, LLC
(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.) Brian R. Strange, 103252 Tel: 310-207-5055 STRANGE & CARPENTER 12100 Wilshire Blvd., Suite 1900, Los Angeles, California 90025	Attorneys (If Known) unknown

II. BASIS OF JURISDICTION (Place an X in one box only.) <input type="checkbox"/> 1 U.S. Government Plaintiff <input type="checkbox"/> 3 Federal Question (U.S. Government Not a Party) <input type="checkbox"/> 2 U.S. Government Defendant <input checked="" type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)	III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only (Place an X in one box for plaintiff and one for defendant.) <table style="width:100%; border: none;"> <tr> <td style="width:30%;"></td> <td style="width:10%; text-align: center;">PTF</td> <td style="width:10%; text-align: center;">DEF</td> <td style="width:40%;"></td> <td style="width:10%; text-align: center;">PTF</td> <td style="width:10%; text-align: center;">DEF</td> </tr> <tr> <td>Citizen of This State</td> <td align="center"><input type="checkbox"/> 1</td> <td align="center"><input type="checkbox"/> 1</td> <td>Incorporated or Principal Place of Business in this State</td> <td align="center"><input type="checkbox"/> 4</td> <td align="center"><input type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td align="center"><input checked="" type="checkbox"/> 2</td> <td align="center"><input type="checkbox"/> 2</td> <td>Incorporated and Principal Place of Business in Another State</td> <td align="center"><input type="checkbox"/> 5</td> <td align="center"><input checked="" type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td align="center"><input type="checkbox"/> 3</td> <td align="center"><input type="checkbox"/> 3</td> <td>Foreign Nation</td> <td align="center"><input type="checkbox"/> 6</td> <td align="center"><input type="checkbox"/> 6</td> </tr> </table>		PTF	DEF		PTF	DEF	Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	<input type="checkbox"/> 4	<input type="checkbox"/> 4	Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 5	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6
	PTF	DEF		PTF	DEF																				
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	<input type="checkbox"/> 4	<input type="checkbox"/> 4																				
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 5																				
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6																				

IV. ORIGIN (Place an X in one box only.)

<input checked="" type="checkbox"/> 1 Original Proceeding	<input type="checkbox"/> 2 Removed from State Court	<input type="checkbox"/> 3 Remanded from Appellate Court	<input type="checkbox"/> 4 Reinstated or Reopened	<input type="checkbox"/> 5 Transferred from another district (specify):	<input type="checkbox"/> 6 Multi-District Litigation	<input type="checkbox"/> 7 Appeal to District Judge from Magistrate Judge
---	---	--	---	---	--	---

V. REQUESTED IN COMPLAINT: JURY DEMAND: ☒ Yes ☐ No (Check 'Yes' only if demanded in complaint.)

CLASS ACTION under F.R.C.P. 23: ☒ Yes ☐ No **MONEY DEMANDED IN COMPLAINT:** \$ over \$5,000,000

VI. CAUSE OF ACTION (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)

This is a class action against Defendants pursuant to the Class Action Fairness Act of 2005, 28 U.S.C., section 1332(d)(2).

VII. NATURE OF SUIT (Place an X in one box only.)

OTHER STATUTES <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce/ICC Rates/etc. <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 810 Selective Service <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 875 Customer Challenge 12 USC 3410 <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Act <input type="checkbox"/> 892 Economic Stabilization Act <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 894 Energy Allocation Act <input type="checkbox"/> 895 Freedom of Info. Act <input type="checkbox"/> 900 Appeal of Fee Determination Under Equal Access to Justice <input type="checkbox"/> 950 Constitutionality of State Statutes	CONTRACT <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	TORTS PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Fed. Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury-Med Malpractice <input type="checkbox"/> 365 Personal Injury-Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 463 Habeas Corpus-Alien Detainee <input type="checkbox"/> 465 Other Immigration Actions	TORTS PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability BANKRUPTCY <input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 CIVIL RIGHTS <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 444 Welfare <input type="checkbox"/> 445 American with Disabilities - Employment <input type="checkbox"/> 446 American with Disabilities - Other <input type="checkbox"/> 440 Other Civil Rights	PRISONER PETITIONS <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 Habeas Corpus General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus/Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition FORFEITURE/PENALTY <input type="checkbox"/> 610 Agriculture <input type="checkbox"/> 620 Other Food & Drug <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 630 Liquor Laws <input type="checkbox"/> 640 R.R. & Truck <input type="checkbox"/> 650 Airline Regs <input type="checkbox"/> 660 Occupational Safety/Health <input type="checkbox"/> 690 Other	LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609
--	--	--	---	---	---

SACV11-01899 AG (JPRx)

FOR OFFICE USE ONLY: Case Number: _____

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

VIII(a). IDENTICAL CASES: Has this action been previously filed in this court and dismissed, remanded or closed? ☒ No ☐ Yes

If yes, list case number(s): _____

VIII(b). RELATED CASES: Have any cases been previously filed in this court that are related to the present case? ☐ No ☒ Yes

If yes, list case number(s): 2:11-cv-10108-CBM-PJW; 2:11-cv-10076-GAF-MRW

Civil cases are deemed related if a previously filed case and the present case:

- (Check all boxes that apply) ☐ A. Arise from the same or closely related transactions, happenings, or events; or
☐ B. Call for determination of the same or substantially related or similar questions of law and fact; or
☐ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
☐ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

IX. VENUE: (When completing the following information, use an additional sheet if necessary.)

(a) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named plaintiff resides.

☐ Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
	Lisa Clark - Oklahoma Felipe Garcia - Texas Robert Spradley - Texas

(b) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named defendant resides.

☐ Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
	Carrier IQ, Inc. - Santa Clara County Samsung Electronics America, Inc. - New Jersey Samsung Telecommunications America, LLC - Texas

(c) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** claim arose.

Note: In land condemnation cases, use the location of the tract of land involved.

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Orange County	

* Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties

Note: In land condemnation cases, use the location of the tract of land involved

X. SIGNATURE OF ATTORNEY (OR PRO PER): _____

Date December 8, 2011

Notice to Counsel/Parties: The CV-71 (JS-44) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))