

FILED  
2011 DEC -9 P 3:41  
RICHARD W. WIEKING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

1 NEWPORT TRIAL GROUP  
2 A Professional Corporation  
3 Scott J. Ferrell, Bar No. 202091  
4 sferrell@trialnewport.com  
5 James B. Hardin, Bar No. 205071  
6 jhardin@trialnewport.com  
7 895 Dove Street, Suite 425  
8 Newport Beach, CA 92660  
9 Tel: (949) 706-6464  
10 Fax: (949) 706-6469

E-filing

11 Attorneys for Plaintiff and the Class

12 UNITED STATES DISTRICT COURT  
13 NORTHERN DISTRICT OF CALIFORNIA

PSG

14 ROSEANNE CASTRO, individually, and on  
15 behalf of all others similarly situated,

Case No. **CV11 6201**

16 Plaintiff,

**CLASS ACTION COMPLAINT**

17 vs.

**JURY TRIAL DEMANDED**

18 CARRIER IQ, INC.; SAMSUNG  
19 ELECTRONICS AMERICA, INC.; SAMSUNG  
20 TELECOMMUNICATIONS AMERICA, INC.;  
21 and DOES 1-25, Inclusive,

22 Defendants.

23 Plaintiff ROSEANNE CASTRO ("Plaintiff"), individually and on behalf of all others similarly  
24 situated, alleges the following on information and belief:

25 **I. INTRODUCTION**

26 1. Plaintiff brings this class action lawsuit based on the unlawful and undisclosed logging  
27 of cell-phone user's activity, including keystrokes, numbers dialed, encrypted web searches and the  
28 contents of text messages on the part of Defendant Carrier IQ, Inc. (hereinafter "Carrier IQ"), as well  
as its cell phone manufacturer partners, Samsung Electronics America, Inc. (hereinafter "Samsung

FAXED  
FIRST LEGAL SUPPORT SERVICES





1 which the matter in controversy exceeds in the aggregate the sum of \$5,000,000, exclusive of interest  
2 and costs.

3 12. Plaintiff alleges that the total damages of the individual members of the Plaintiff Class  
4 in this action are in excess of \$5,000,000 in the aggregate, exclusive of interest and costs, as required  
5 by 28 U.S.C. § 1332(d)(2), (5). Further, as set forth above, Plaintiff is a citizen of California and  
6 Defendants are citizens of Delaware, Texas, New York and/or New Jersey. Therefore, diversity of  
7 citizenship exists under CAFA, as required by 28 U.S.C. § 1332(d)(2)(A).

#### 8 IV. FACTS

9 13. Defendant Carrier IQ's software is a rootkit software system which is automatically  
10 included on certain carriers' cellular phones and devices, including the one used by Plaintiff and Class  
11 Members. "Rootkit" software is a kind of software that enables continued access to a computer or  
12 cellular device while actively hiding its presence from administrators by subverting standard operating  
13 system functionality or other applications. In other words, Carrier IQ is a software system and  
14 application included in cellular devices which is purposefully hidden from users and enables  
15 Defendants to track certain uses of the cell or smart-phone device. This software is difficult for the  
16 unsophisticated user to find and cannot be removed or deactivated by the user, unlike standard  
17 software applications like Facebook or Adobe.

18 14. Last month computer programmer Trevor Eckhart posted a video on Youtube.com  
19 detailing the ways Defendant Carrier IQ uses its rootkit software to track and record the personal  
20 information of mobile device users without their knowledge or consent.<sup>1</sup> The video quickly became  
21 viral and prompted extreme outrage and discomfort from those users who have mobile devices  
22 containing the Carrier IQ software which was neither disclosed to them, nor authorized by them.  
23 Perhaps more importantly, the video detailed the fact that users have no ability to remove or opt-out of  
24 the program which is automatically installed on their phone.

25 15. What is also so troubling about the Carrier IQ software, aside from the fact that users  
26 have absolutely no control over its function and use, is that it has the ability to track extremely  
27

28 <sup>1</sup> [http://www.youtube.com/watch?v=T17XQI\\_AYNo](http://www.youtube.com/watch?v=T17XQI_AYNo).

1 personal and private information about the cellular or smart-phone user including their location,  
2 incoming and outgoing calls, contents of text messages, both encrypted and unencrypted internet web-  
3 searches, network connectivity, blue-tooth connection, and numerous other key-stroke activities. So,  
4 for example, Defendant Carrier IQ can gain a user's bank name, their login name and password, even  
5 if the website is encrypted, or collect users' private information sent via text message, or determine  
6 where a user is calling from or calling to. All of this private collection of users' data is not disclosed  
7 to users at any point including upon purchase, enabling the device, or when logging into assumed-to-  
8 be private internet locations via their phone. Just as there is no disclosure, there is likewise no consent  
9 or authorization sought from users. The result is a cellular or smart-phone device that collects and  
10 stores personal, private information from its user with absolutely no disclosure, authorization or notice  
11 as to what the private information is being used for.

12 16. Defendant Carrier IQ claims that they are the "leading provider in Mobile Service  
13 Intelligence Solutions" and that they "give to their Wireless Carriers and Handset Manufacturers  
14 **unprecedented insight into their customers' mobile experience.**"<sup>2</sup> Defendant Carrier IQ further  
15 claims that those who use their Mobile Service Intelligence solution, such as the Samsung Defendants,  
16 can "eliminate[] guesswork by **automatically providing accurate, real-time data direct from the**  
17 **source – your customers' handsets.** Our powerful platform aggregates, analyzes and delivers that  
18 data via easy-to-use web applications that help wireless carriers make smart business decisions."<sup>3</sup>  
19 Defendant Carrier IQ admits to embedding diagnostic software in millions of subscribers' phones so  
20 that wireless carriers can determine "exactly how [their] customers interact with services and which  
21 ones they use... [as well as] see which content they consume, **even offline.**"<sup>4</sup>

22 17. After the Eckhart video went viral and consumer outrage ballooned, Carrier IQ  
23 responded by denying that its software recorded keystrokes and insisted that it only measured and  
24 summarized cellphone performance, yet when Carrier IQ's marketing manager, Andrew Coward was  
25 asked by Wired Magazine if Carrier IQ could read users' text messages if it wanted to, Coward  
26

27 <sup>2</sup> <http://www.carrieriq.com/> (emphasis added).

28 <sup>3</sup> <http://www.carrieriq.com/overview/index.htm> (emphasis added).

<sup>4</sup> <http://www.carrieriq.com/overview/IQInsightExperienceManager/index.htm> (emphasis added).

1 responded, "probably, yes."<sup>5</sup> In addition, Defendant Carrier IQ reacted to Eckhart's video by issuing a  
2 cease and desist demand letter on November 18, 2011, threatening Eckhart with legal action based on  
3 his alleged "willful infringement" of United States copyright laws. (A copy of the redacted cease and  
4 desist demand letter is attached hereto as Exhibit A). Carrier IQ later withdrew their threats of legal  
5 action when Mr. Eckhart sought counsel with the Electronic Frontier Foundation.

6  
7 18. The reaction of outrage to Defendant Carrier IQ's infringement upon users' privacy  
8 spread so far as to receive a reaction from the United States Senate Judiciary Committee. In a letter to  
9 Defendant Carrier IQ's President and CEO Larry Lenhart, Senator Al Franken expressed the common  
10 concerns and reactions upon learning about Carrier IQ's use of users' private information. In pertinent  
11 part, Senator Franken stated: "Consumers need to know that their safety and privacy are being  
12 protected by the companies they trust with their sensitive information. The revelation that the  
13 locations and other sensitive data of millions of Americans are being secretly recorded and possibly  
14 transmitted is deeply troubling. This news underscores the need for Congress to act swiftly to protect  
15 the location information and private, sensitive information of consumers. But right now, Carrier IQ has  
16 a lot of questions to answer." (A copy of the Senate Judiciary letter is attached hereto as Exhibit B).

17 19. To date, Defendant Carrier IQ has made no adjustments as to how and to what data they  
18 collect from their wireless carrier partners' users. Defendant Carrier IQ's software is installed in over  
19 141 million devices and counting. As such, Plaintiff and class bring this lawsuit to enjoin the  
20 Defendants from their ongoing infringement of privacy rights and to recover the damages from this  
21 illegal and unauthorized activity.

#### 22 **V. CLASS ACTION ALLEGATIONS**

23 20. This action is properly maintainable as a class action under Federal Rules of Civil  
24 Procedure 23(b)(1), 23(b)(2) and/or 23(b)(3). Plaintiff brings this class action for damages and other  
25 monetary relief on behalf of the following classes:

26 a. Carrier IQ Subclass:

27  
28 <sup>5</sup> <http://www.wired.com/threatlevel/2011/11/rootkit-brouhaha/> (last visited December 4, 2011).

1 All persons located within the United States who used a mobile  
2 device with Carrier IQ software installed ("Carrier IQ Subclass").

3 b. Samsung Subclass:

4 All persons located within the United States who used a Samsung Electronics or  
5 Telecommunications mobile device with Carrier IQ software installed ("Samsung  
6 Communications Subclass").

7  
8 21. Excluded from the Class are governmental entities, Defendants, any entity in which  
9 defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal  
10 representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from  
11 the Class is any judge, justice, or judicial officer presiding over this matter and the members of their  
12 immediate families and judicial staff.

13 22. The proposed Class is so numerous that individual joinder of all its members is  
14 impracticable. Due to the nature of the trade and commerce involved, however, Plaintiff believes that  
15 the total number of Class members is in the millions and members of the Class as numerous and  
16 geographically dispersed across the United States. While the exact number and identities of the Class  
17 members are unknown at this time, such information can be ascertained through appropriate  
18 investigation and discovery. The disposition of the claims of the Class members in a single class  
19 action will provide substantial benefits to all parties and to the Court.

20 23. There is a well-defined community of interest in the questions of law and fact involved  
21 affecting the Plaintiff Class and these common questions predominate over any questions that may  
22 affect individual Class members. Common questions of fact and law include, but are not limited to,  
23 the following:

24 a. Whether Defendants recorded, tracked, and/ or stored private information from  
25 the Plaintiff's and Classes' mobile devices;

26 b. Whether Defendants knew they were recording, tracking and/ or storing private  
27 information of the Plaintiff and Classes;

28 c. Whether Defendants made false and misleading statements about recording,  
tracking and/ or storing private information of the Plaintiff and Class;

1           d.     Whether Defendants' conduct violates the Federal Wiretap Act (18 U.S.C. §§  
2 2511, *et seq.*);

3           e.     Whether Defendants' conduct violates the Computer Fraud and Abuse Act (18  
4 U.S.C. §§ 1030, *et seq.*);

5           f.     Whether Defendants' conduct violates Section 631 of the California Penal  
6 Code;

7           g.     Whether Defendants' conduct violates Section 632.7 of the California Penal  
8 Code;

9           h.     Whether Defendants are liable for damages pursuant to Section 637.2 of the  
10 California Penal Code;

11          i.     Whether Plaintiffs and the Class are entitled to statutory, exemplary, and  
12 compensatory damages, and if so, to what amount they are entitled; and

13          j.     Whether Carrier IQ should be ordered to disgorge all or part of the ill-gotten  
14 gains it received from the sale of the Carrier IQ software, and/or to make full restitution to  
15 Plaintiffs and the Class.

16  
17           These common questions of law and fact predominate over questions that may affect individual  
18 Class members in that the claims of all Class members for each of the claims herein can be established  
19 with common proof. Additionally, a class action would be "superior to other available methods for the  
20 fair and efficient adjudication of the controversy," as set forth in Rule 23(b)(3) of the Federal Rules of  
21 Civil Procedure in that (1) Class members have little interest in individually controlling the  
22 prosecution of separate actions because the individual damages claims of each Class member are not  
23 substantial enough to warrant individual filings; (2) Plaintiff is not aware of any other lawsuits against  
24 Defendants commenced by or on behalf of members of the Class; and (3) because the recording,  
25 tracking, and storing of mobile device users' private information are common to all Class members  
26 and because resolution of the claims of Plaintiff will resolve the claims of the remaining Class,  
27 certification does not pose any manageability problems. Notice may be given by publication.  
28



1           24. Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and all  
2 members of the Class have been similarly affected by Defendants' common course of conduct since  
3 they all were subject to Defendants' recording, tracking, and storing of private information contained  
4 on their mobile devices.

5           25. Plaintiff will fairly and adequately represent and protect the interests of the Class.  
6 Plaintiff has retained counsel with substantial experience in handling complex class action litigation.  
7 Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the Class and  
8 have the financial resources to do so. Plaintiff has retained a law firm who is widely recognized as one  
9 of the most successful and effective class action litigators in California, and whose victories have been  
10 publicized on CNN, Fox News, MSNBC, and nearly every major California newspaper. The firm has  
11 also been certified as lead class counsel in other class actions. (*See e.g., DeLaRosa v. Boiron, Inc.*,  
12 Case No. 8:10-CV-1569-JST (CWx) (C.D. Cal.).

13           26. Plaintiff and the members of the Class suffered, and will continue to suffer, harm as a  
14 result of Defendants' unlawful and wrongful conduct. A class action is superior to other available  
15 methods for the fair and efficient adjudication of the present controversy. Individual joinder of all  
16 members of the class is impracticable. Even if individual class members had the resources to pursue  
17 individual litigation, it would be unduly burdensome to the courts in which the individual litigation  
18 would proceed. Individual litigation magnifies the delay and expense to all parties in the court system  
19 of resolving the controversies engendered by Defendants' common course of conduct. The class  
20 action device allows a single court to provide the benefits of unitary adjudication, judicial economy,  
21 and the fair and efficient handling of all class members' claims in a single forum. The conduct of this  
22 action as a class action conserves the resources of the parties and of the judicial system and protects  
23 the rights of the class members. Furthermore, for many, if not most, a class action is the only feasible  
24 mechanism that allows an opportunity for legal redress and justice.

25           27. Adjudication of individual class members' claims with respect to Defendants would, as  
26 a practical matter, be dispositive of the interests of other members not parties to the adjudication, and  
27 could substantially impair or impede the ability of other class members to protect their interests.  
28

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

**VI. CAUSES OF ACTION**

**FIRST CAUSE OF ACTION**

**VIOLATION OF FEDERAL WIRETAP ACT (18 U.S.C. §§ 2511, et seq.)**

28. Plaintiff and subclasses incorporate by this reference the allegations contained in the preceding paragraphs as if fully set forth herein and, to the extent necessary, pleads this cause of action in the alternative.

29. This cause of action is brought on behalf of Plaintiff Roseanne Castro and the Carrier IQ subclass against Defendant Carrier IQ; and Plaintiff Roseanne Castro and the Samsung Subclass against Defendants Samsung Electronics, Samsung Telecommunications and Carrier IQ.

30. Defendants intentionally intercepted, endeavored to intercept, and/ or procured electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. §§ 2511, *et seq.* (the "Federal Wiretap Act"). In addition, Defendants intentionally used, endeavored to use, and/ or procured the electronic communications of Plaintiff and Class Members, knowing or having reason to know that the information was obtained through the interception of an electronic communication, in violation of the Federal Wiretap Act.

31. Defendants intercepted electronic communications which were not accessible to the general public through an electronic communication system. Those electronic communications intercepted by Defendants were private and confidential to Plaintiff and Class Members.

32. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members are each entitled to the following based on Defendants' conduct: (1) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000 per Class Member; (2) punitive damages; (3) injunctive or declaratory relief as deemed appropriate; and (4) reasonable attorneys' fees and costs.

**SECOND CAUSE OF ACTION**

**VIOLATION OF COMPUTER FRAUD AND**

**ABUSE ACT, (18 U.S.C. §§ 1030, et seq.)**

33. Plaintiff and subclasses incorporate by this reference the allegations contained in the preceding paragraphs as if fully set forth herein and, to the extent necessary, pleads this cause of

1 action in the alternative.

2 34. This cause of action is brought on behalf of Plaintiff Roseanne Castro and the Carrier  
3 IQ subclass against Defendant Carrier IQ; and Plaintiff Roseanne Castro and the Samsung Subclass  
4 against Defendants Samsung Electronics, Samsung Telecommunications and Carrier IQ.

5 35. Plaintiff's and Class Members' mobile devices using the Carrier IQ software are  
6 "computers" within the meaning of 18 U.S.C. § 1030(e)(1) because they are high speed data  
7 processing devices that perform logical, arithmetic, or storage functions and include data storage  
8 facilities or communications facilities directly related to or operating in conjunction with such device.  
9 Further, Plaintiff's and Class Members' mobile devices are "protected computers" within the meaning  
10 of 18 U.S.C. § 1030(e)(2)(B) because they are used in interstate commerce or communication.

11 36. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030, *et*  
12 *seq.*, by, *inter alia*: (1) knowingly and intentionally accessing Plaintiff's and Class Members' mobile  
13 devices without authorization or exceeding authorized access, thereby obtaining protected information  
14 from their mobile devices; (2) knowingly causing the transmission of a program, information, code, or  
15 command, and as a result of such conduct, intentionally causes damage without authorization, to  
16 Plaintiff's and Class Members' mobile devices; (3) intentionally accessing Plaintiff's and Class  
17 Members' mobile devices without authorization, and as a result, recklessly causing damage; and/or (4)  
18 intentionally accessing Plaintiff's and Class Members' mobile devices without authorization, and as a  
19 result, causing damage and loss.

20 37. Defendants, without authorization or in excess of their authorized access, knowingly  
21 and intentionally accessed Plaintiff's and Class Members' mobile devices to obtain protected  
22 information from their mobile devices. Defendants recorded, tracked and stored the private  
23 information from Plaintiff's and Class Members' mobile devices specifically obtaining Plaintiff's and  
24 Class Members' locations, text messages, telephone numbers going in and out, encrypted and  
25 unencrypted website searches, and other keystroke information.

26 38. Defendants, without authorization, knowingly and intentionally accessed Plaintiff's and  
27 Class Members' mobile devices, recklessly causing damage by interfering with protected information,  
28 data, and communications and placed at risk Plaintiff's and Class Members' private and confidential

1 information and communications.

2 39. Defendants' knowing and intentional conduct directly caused damages affecting ten or  
3 more protected computers during a one-year period exceeding an aggregate amount of \$5,000 in  
4 damages.

5 **THIRD CAUSE OF ACTION**

6 **VIOLATION OF CALIFORNIA PENAL CODE SECTION 631**

7 40. Plaintiff and subclasses incorporate by this reference the allegations contained in the  
8 preceding paragraphs as if fully set forth herein and, to the extent necessary, pleads this cause of  
9 action in the alternative.

10 41. This cause of action is brought on behalf of Plaintiff Roseanne Castro and the Carrier  
11 IQ subclass against Defendant Carrier IQ; and Plaintiff Castro and the Samsung Subclass against  
12 Defendants Samsung Electronics, Samsung Telecommunications and Carrier IQ.

13 42. Pursuant to California Penal Code § 631, it is unlawful for any person to intentionally  
14 tap, or make an unauthorized connection with any telegraph or telephone, or to willfully and without  
15 the consent of all parties to the communication, attempt to read, or to learn the contents or meaning of  
16 any message or communication while the same is in transit or passing over any wire, line, or cable, or  
17 is being sent.

18 43. Defendants have violated California Penal Code § 631 by recording, tracking, and/ or  
19 storing private and confidential information from Plaintiff's and Class Members' mobile devices  
20 without authorization. Defendants' use the Carrier IQ software to record, track, and/ or store the  
21 keystrokes made by Plaintiff and Class Members on their mobile devices, thereby collecting  
22 information relating to locations, text messages, telephone numbers going in and out, encrypted and  
23 unencrypted website searches, and other keystroke information.

24 44. Defendants' conduct constitutes an intentional tapping in violation of California Penal  
25 Code § 631 because users are unaware of the Carrier IQ software on their mobile device, do not have  
26 the ability to consent to or authorize it, and cannot disable or turn off the software. In addition,  
27 Defendants' conduct constitutes the unauthorized reading or learning, or attempt to read, messages,  
28 reports or communications in violation of California Penal Code § 631. Plaintiff and Class Members

1 have been injured by Defendants' conduct because private and confidential information has been  
2 recorded, tracked and/ or stored by Defendants without knowledge, consent, or authorization thereby  
3 placing at risk that private and confidential information.

4 45. Civil actions for violations of California Penal Code § 631 are permitted by California  
5 Penal Code § 637.2 which authorizes an award of \$5,000 for each violation as well as injunctive relief.  
6 Plaintiff and Class Members are entitled to these remedies and attorneys' fees as this lawsuit seeks the  
7 enforcement of an important right affecting the public interest and satisfies the statutory requirements  
8 for an award of attorneys' fees thereunder.

9 46. Plaintiffs and Class Members have sustained and will continue to sustain injury based  
10 on Defendants' conduct and seek both injunctive relief and statutory damages to be determined at trial.

11 **FOURTH CAUSE OF ACTION**

12 **VIOLATION OF CALIFORNIA PENAL CODE SECTION 632.7**

13 47. Plaintiff and subclasses incorporate by this reference the allegations contained in the  
14 preceding paragraphs as if fully set forth herein and, to the extent necessary, pleads this cause of  
15 action in the alternative.

16 48. This cause of action is brought on behalf of Plaintiff Roseanne Castro and the Carrier  
17 IQ subclass against Defendant Carrier IQ; and Plaintiff Roseanne Castro and the Samsung Subclass  
18 against Defendants Samsung Electronics, Samsung Telecommunications and Carrier IQ.

19 49. Pursuant to California Penal Code § 632.7, the intentional, non-consensual  
20 eavesdropping or recording of the confidential communications of parties to a confidential  
21 communication, is prohibited.

22 50. Defendants have violated California Penal Code § 632.7 by intentionally, and without  
23 the consent of all parties to the communications, recorded, tracked, and/ or stored confidential  
24 communications including but not limited to text messages and emails by Plaintiff and Class Members  
25 on their mobile devices.

26 51. Plaintiff and Class Members have been injured by Defendants' intentional and non-  
27 consensual conduct in that their confidential and private communications have been recorded, tracked,  
28 and/ or stored, thereby placing at risk that confidential and private communication.




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

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a trial by jury of all claims and causes of action so triable in this lawsuit.

Dated: December 9, 2011

NEWPORT TRIAL GROUP  
A Professional Corporation  
Scott J. Ferrell

By:   
Scott J. Ferrell

Attorney for Plaintiff and the Class

## CEASE AND DESIST DEMAND

Sent by Certified Mail and email

November 16, 2011

Trevor Eckhart

[REDACTED]

[REDACTED]

[REDACTED]

Dear Mr. Eckhart:

I am writing on behalf on my employer, Carrier IQ, Inc., to notify you that your unlawful copying of Carrier IQ, Inc.'s training materials on your website<sup>1</sup> (the "Training Materials") infringes on Carrier IQ, Inc.'s exclusive copyrights. Accordingly, you are hereby directed to

### CEASE AND DESIST ALL COPYRIGHT INFRINGEMENT.

All copyrightable aspects of the Training Materials are copyrighted under United States copyright law and Carrier IQ, Inc. is the owner of such copyright. Under United States copyright law, Carrier IQ, Inc.'s copyrights have been in effect since the date that the Training Materials were created.

It has come to our attention that you have been copying the Training Materials. We have copies of your unlawful copies to preserve as evidence. Your actions constitute copyright infringement in violation of United States copyright laws. Under 17 U.S.C. 504, the consequences of copyright infringement include statutory damages of between \$750 and \$30,000 per work, at the discretion of the court, and damages of up to \$150,000 per work for willful infringement. If you continue to engage in copyright infringement after receiving this letter, your actions will be evidence of "willful infringement."

### CEASE AND DESIST ALL FALSE ALLEGATIONS.

In addition to infringing Carrier IQ, Inc.'s copyrights, you have made allegations on your website (see footnote 1), that are without substance, untrue, and that we regard as

<sup>1</sup> <http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/> ;  
<http://www.androidfilehost.com/main/TrevE/CIQ/>

JSD



## CEASE AND DESIST DEMAND

damaging to our reputation and the reputation of our customers. At this time we demand that you remove such allegations from the web and cease and desist from making any allegations or passing any false and unsubstantiated public comment directly or indirectly on our company, products, services or companies who may use our technology.

### We demand that you immediately

- cease and desist your unlawful copying of the Training Materials;
- contact all persons and entities to whom you have directly or indirectly provided copies of the Training Materials and inform them that such materials are confidential/copyright-protected materials belonging to Carrier IQ, Inc. were provided improperly in infringement of the rights of Carrier IQ, Inc.;
- provide Carrier IQ, Inc. with contact information for such all persons and entities;
- cease and desist from making any unsubstantiated allegations or passing any false or unsubstantiated public comment directly or indirectly relating to Carrier IQ, Inc., its products and services or companies who may use Carrier IQ, Inc. technology;
- send written retractions to all persons and entities to whom you have directly or indirectly distributed the unsubstantiated allegations relating to Carrier IQ, Inc. products or services;
- issue a public press release on the AP wire containing the following statement:
- remove all content and references to Carrier IQ, Inc. (including references to Carrier IQ and/or CIQ) from the website androidsecuritytest.com, any mirrors and references and replace your original "CarrierIQ" article with the following statement:

"Carrier IQ, Inc. has requested that I remove my original article entitled "CarrierIQ" as it contained numerous inaccuracies and material subject to their copyright. I would also like to apologize to Carrier IQ, Inc. for misrepresenting the capabilities of their products and for distributing copyrighted content without permission.

"On clarifying the actions of Carrier IQ, Inc. software, it is clear that while they inspect many aspects of device performance they are not in fact recording keystrokes or providing user tracking tools and have no intention of doing so.

"Carrier IQ, Inc. technology does not allow their customers to task devices which are no longer in their service (for example when a subscriber of one operator moves their phone to another operator) and restricts each customer to its own subscribers.

"The Carrier IQ, Inc. software is integrated by intent by device manufacturers and operators; it does not meet the definition of a rootkit and does not subvert the operation of the device as I previously claimed. Under my previous

JJD

## CEASE AND DESIST DEMAND

definition, any software loaded by an OEM that shipped with a device would meet my criteria for rootkit.”

- provide Carrier IQ, Inc. with prompt written assurance by 12.00pm EST on November 18th that you will comply with the foregoing.

If you do not comply with these cease and desist demands within this time period, please be advised that Carrier IQ, Inc. will pursue all available legal remedies; including seeking monetary damages, injunctive relief, and an order that you pay court costs and attorney's fees. In addition, Carrier IQ, Inc. is entitled to use your failure to comply as evidence of “willful infringement” of copyright and seek monetary damages and equitable relief for your copyright infringement. In the event you fail to meet this demand, your liability and exposure under such legal action could be considerable.

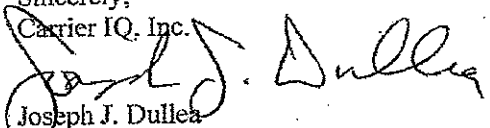
Before taking these steps, however, Carrier IQ, Inc. wishes to give you one opportunity to discontinue your illegal conduct by complying with this demand by 12.00pm EST on November 18th. Accordingly, please sign and return the attached *Agreement* by 12.00pm EST on November 18th to

Joseph J. Dullea  
c/o Jewel Rich  
1200 Villa St., Suite 200  
Mountain View, CA 94041

With an email copy to [REDACTED]@carrieriq.com, cc [REDACTED]@carrieriq.com

If you or your attorney have any questions, please contact me directly.

Sincerely,  
Carrier IQ, Inc.

  
Joseph J. Dullea  
General Counsel  
[REDACTED]

## CEASE AND DESIST DEMAND

Attached page:

### Copyright Infringement Settlement Agreement

I, \_\_\_\_\_, agree to immediately:

- cease and desist your unlawful copying of the Training Materials;
- contact all persons and entities to whom you have directly or indirectly provided copies of the Training Materials and inform them that such materials are confidential/copyright-protected materials belonging to Carrier IQ, Inc. were provided improperly in infringement of the rights of Carrier IQ, Inc.;
- provide Carrier IQ, Inc. with contact information for such all persons and entities;
- cease and desist from making any unsubstantiated allegations or passing any false or unsubstantiated public comment directly or indirectly relating to Carrier IQ, Inc., its products and services or companies who may use Carrier IQ, Inc. technology;
- send written retractions to all persons and entities to whom you have directly or indirectly distributed the unsubstantiated allegations relating to Carrier IQ, Inc. products or services;
- issue a public press release on the AP wire containing the following statement:
- remove all content and references to Carrier IQ, Inc. (including references to Carrier IQ and/or CIQ) from the website androidsecuritytest.com, any mirrors and references and replace your original "CarrierIQ" article with the following statement:

"Carrier IQ, Inc. has requested that I remove my original article entitled "CarrierIQ" as it contained numerous inaccuracies and material subject to their copyright. I would also like to apologize to Carrier IQ, Inc. for misrepresenting the capabilities of their products and for distributing copyrighted content without permission.

"On clarifying the actions of Carrier IQ, Inc. software, it is clear that while they inspect many aspects of device performance they are not in fact recording keystrokes or providing user tracking tools and have no intention of doing so.

"Carrier IQ, Inc. technology does not allow their customers to task devices which are no longer in their service (for example when a subscriber of one operator moves their phone to another operator) and restricts each customer to its own subscribers.

"The Carrier IQ, Inc. software is integrated by intent by device manufacturers and operators; it does not meet the

## CEASE AND DESIST DEMAND

definition of a rootkit and does not subvert the operation of the device as I previously claimed. Under my previous definition, any software loaded by an OEM that shipped with a device would meet my criteria for rootkit.”

in exchange for which Carrier IQ, Inc. agrees to release any claims against me for copyright infringement with respect to the Training Materials. In the event this agreement is breached by me, Carrier IQ, Inc. will be entitled to costs and attorney’s fees in any action brought to enforce this agreement and shall be free to pursue all rights that Carrier IQ, Inc. had as of the date of this Agreement as if this Agreement had never been signed.

Signed: \_\_\_\_\_

Dated: \_\_\_\_\_

JJD

PATRICK J. LEAHY, VERMONT, CHAIRMAN

HERB KOHL, WISCONSIN  
DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHELDON WHITEHOUSE, RHODE ISLAND  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. COONS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT

CHARLES E. GRASSLEY, IOWA  
ORRIN G. HATCH, UTAH  
JON KYL, ARIZONA  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TOM COBURN, OKLAHOMA

## United States Senate

COMMITTEE ON THE JUDICIARY  
WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Chief Counsel and Staff Director*  
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

November 30, 2011

Mr. Larry Lenhart, President and CEO  
Carrier IQ, Inc.  
1200 Villa Street, Suite 200  
Mountain View, CA 94041

Dear Mr. Lenhart,

I am very concerned by recent reports that your company's software—pre-installed on smartphones used by millions of Americans—is logging and may be transmitting extraordinarily sensitive information from consumers' phones, including:

- when they turn their phones on;
- when they turn their phones off;
- the phone numbers they dial;
- the contents of text messages they receive;
- the URLs of the websites they visit;
- the contents of their online search queries—even when those searches are encrypted; and
- the location of the customer using the smartphone—even when the customer has *expressly denied* permission for an app that is currently running to access his or her location.

It appears that this software runs automatically every time you turn your phone on. It also appears that an average user would have no way to know that this software is running—and that when that user finds out, he or she will have no reasonable means to remove or stop it.

These revelations are especially concerning in light of Carrier IQ's public assertions that it is "not recording keystrokes or providing tracking tools" (November 16), "[d]oes not record your keystrokes," and "[d]oes not inspect or report on the content of your communications, such as the content of emails and SMSs" (November 23).


I understand the need to provide usage and diagnostic information to carriers. I also understand that carriers can modify Carrier IQ's software. But it appears that Carrier IQ's software captures a broad swath of extremely sensitive information from users that would appear to have nothing to do with diagnostics—including who they are calling, the *contents* of the texts they are receiving, the *contents* of their searches, and the websites they visit.

These actions may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. This is potentially a very serious matter.

I ask that you provide answers to the following questions by December 14, 2011.

- (1) Does Carrier IQ software log users' location?
- (2) What other data does Carrier IQ software log? Does it log:
  - a. The telephone numbers users dial?
  - b. The telephone numbers of individuals calling a user?
  - c. The contents of the text messages users receive?
  - d. The contents of the text messages users send?
  - e. The contents of the emails they receive?
  - f. The contents of the emails users send?
  - g. The URLs of the websites that users visit?
  - h. The contents of users' online search queries?
  - i. The names or contact information from users' address books?
  - j. Any other keystroke data?
- (3) What if any of this data is transmitted off of a users' phone? When? In what form?
- (4) Is that data transmitted to Carrier IQ? Is it transmitted to smartphone manufacturers, operating system providers, or carriers? Is it transmitted to any other third parties?
- (5) If Carrier IQ receives this data, does it subsequently share it with third parties? With whom does it share this data? What data is shared?
- (6) Will Carrier IQ allow users to stop any logging and transmission of this data?
- (7) How long does Carrier IQ store this data?
- (8) Has Carrier IQ disclosed this data to federal or state law enforcement?
- (9) How does Carrier IQ protect this data against hackers and other security threats?
- (10) Does Carrier IQ believe that its actions comply with the Electronic Communications Privacy Act, including the federal wiretap statute (18 U.S.C. § 2511 et seq.), the pen register statute (18 USC § 3121 et seq.), and the Stored Communications Act (18 U.S.C. § 2701 et seq.)?
- (11) Does Carrier IQ believe that its actions comply with the Computer Fraud and Abuse Act (18 U.S.C. § 1030)? Why?

I appreciate your prompt attention to this matter.

Sincerely,  
  
AL FRANKEN  
Chairman, Subcommittee on Privacy  
Technology and the Law