

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

SHANA E. SCARLETT (217895)  
HAGENS BERMAN SOBOL SHAPIRO LLP  
715 Hearst Avenue, Suite 202  
Berkeley, CA 94710  
Telephone: (510) 725-3000  
Facsimile: (510) 725-3001  
shanas@hbsslaw.com

STEVE W. BERMAN, *pro hac vice* (application pending)  
ROBERT F. LOPEZ, *pro hac vice* (application pending)  
THOMAS E. LOESER (202724)  
HAGENS BERMAN SOBOL SHAPIRO LLP  
1918 Eighth Avenue, Suite 3300  
Seattle, WA 98101  
Telephone: (206) 623-7292  
Facsimile: (206) 623-0594  
steve@hbsslaw.com  
robl@hbsslaw.com  
toml@hbsslaw.com

*Attorneys for Plaintiffs and the Proposed Class*

**E-filing**

**HRL**

**FILED**

DEC - 2 2011

RICHARD W. WIEKING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

**3 FAXED**

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

No. **11** **5819**

ERIC THOMAS, a Texas resident, and  
BENJAMIN LANCASTER, a Pennsylvania  
resident, on behalf of themselves and all others  
similarly situated,

Plaintiffs,

v.

CARRIER IQ, INC., a Delaware corporation;  
SAMSUNG ELECTRONICS CO., LTD., a  
Korean company,  
SAMSUNG ELECTRONICS AMERICA, Inc. a  
New York corporation, and  
SAMSUNG TELECOMMUNICATIONS  
AMERICA, INC., a Delaware corporation,

Defendants.

CLASS ACTION COMPLAINT

1. VIOLATION OF FEDERAL  
WIRETAP ACT AS AMENDED BY  
THE ELECTRONIC  
COMMUNICATIONS PRIVACY  
ACT, 18 U.S.C. §§ 2510 *et seq.*

2. VIOLATION OF UNFAIR  
BUSINESS PRACTICES ACT [CAL.  
BUS. & PROF. CODE §§ 17200, *ET  
SEQ.*]

**DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

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

I. INTRODUCTION..... 1

II. JURISDICTION..... 1

III. PARTIES..... 2

IV. FACTUAL BACKGROUND ..... 3

    A. Carrier IQ ..... 3

    B. Discovery of Carrier IQ’s interception of electronic communications ..... 4

    C. Plaintiffs’ Cellular Devices Were Embedded With Carrier IQ Software and Their  
        Communications Were Intercepted Without Authorization..... 8

V. CLASS ALLEGATIONS..... 9

VI. CLAIMS FOR RELIEF ..... 11

    COUNT I VIOLATION OF THE FEDERAL WIRETAP ACT..... 11

    COUNT II VIOLATION OF THE UNFAIR COMPETITION LAW (CAL. BUS. &  
        PROF. CODE §§ 17200 *et seq.*) ..... 12

VII. PRAYER FOR RELIEF ..... 13

VIII. JURY TRIAL DEMANDED ..... 14

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

## I. INTRODUCTION

1. Defendant Carrier IQ, Inc. (“CIQ” or “Carrier IQ”) created and provides software that is embedded on cellular devices manufactured by HTC Corporation; HTC America, Inc.; and Defendants Samsung Electronics, Inc.; Samsung Electronics America, Inc.; and Samsung Telecommunications America, Inc. (the “Device Manufacturers”). CIQ touts its software as a tool for cellular carriers and device manufacturers to improve end-user experience on cellular devices. CIQ claims that its software does not log key-strokes and thus does not intercept, store, and transfer consumer’s electronic communications to third parties, *i.e.*, cellular carriers and device manufacturers.

2. In truth and fact, however, CIQ software does log keystrokes and does store and transmit to third parties detailed information, including the content of user messages sent and received.

3. Consumers using devices equipped with CIQ software are not notified that the software is actively running on their devices and have no idea that, and give no consent for, their private communications to be intercepted, stored, and transmitted to third parties.

4. By embedding the CIQ software in cellular and other devices that are sold to consumers whose electronic communications are then intercepted, stored, and transmitted by way of that software, Defendant CIQ and the Defendant Device Manufacturers engage in direct violations of federal wiretap law, as well as applicable state law.

5. Through this action, Plaintiffs seek to stop Defendants’ unauthorized and illegal interception of electronic communications and to recover damages and other relief prescribed by law.

## II. JURISDICTION

6. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 in that Plaintiffs allege violations of federal law, namely the Federal Wiretap Act as amended by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* The Court has supplemental jurisdiction over Plaintiffs’ state law claims pursuant to 28 U.S.C. § 1367(a).



1 SEC has offices within the United States and California and sells its products throughout the  
2 United States, including throughout California.

3 16. SEA, STA, and SEC are collectively referred to as "Samsung."

#### 4 IV. FACTUAL BACKGROUND

##### 5 A. Carrier IQ

6 17. On its website<sup>1</sup> under the heading, "Who we are," Carrier IQ states:

7 Carrier IQ is the world's leading provider of Mobile Service Intelligence  
8 solutions. Founded in 2005 and with a management team steeped in the mobile  
9 telecoms industry, the company is privately held and funded by some of the leading  
10 players in the venture capital industry. Carrier IQ is headquartered in Mountain  
11 View, California with additional offices in Chicago, Boston, London (UK) and  
12 Kuala Lumpur (Malaysia). Our mission is to provide mobile carriers and device  
13 OEMs with unprecedented insight into service performance and usability and so  
14 enable them to deliver higher quality products and services to their customers.

15 18. Under the heading, "What we do," Carrier IQ touts its ability to track and deliver  
16 "data drawn directly from your subscribers' devices" to provide "detailed insight into the mobile  
17 experience as delivered at the handset. . . ." It states:

18 Carrier IQ is the market leader in Mobile Service Intelligence solutions that  
19 have revolutionized the way mobile operators and device vendors gather and  
20 manage information from end users. With Carrier IQ's unique ability to provide  
21 detailed insight into service delivery and user experience, you can achieve your  
22 strategic goals more efficiently and effectively, based on data drawn directly from  
23 your subscribers' devices – the place where your customer actually experiences the  
24 service.

25 The Carrier IQ solution goes beyond traditional point offerings that address  
26 a single business problem, to provide a comprehensive Mobile Service Intelligence  
27 platform which builds upon underlying customer experience data to enable all areas  
28 of your business to operate more effectively: from planning to operations, from  
marketing to customer care.

Recognizing the phone as an integral part of a mobile service delivery, and  
using the device to measure key parameters of service quality and usage, the Carrier  
IQ solution gives you the unique ability to analyze in detail usage scenarios and  
fault conditions by type, location, application and network performance while  
providing you with a detailed insight into the mobile experience as delivered at the  
handset rather than simply the state of the network components carrying it.

The resulting unprecedented insight allows you to manage your business directly to  
KPIs based on your customer's experience, not just system statistics.

<sup>1</sup> [www.carrieriq.com/company/index.htm](http://www.carrieriq.com/company/index.htm) (last accessed November 30, 2011).

1 19. Acknowledging the serious implications of its interception, storage, and delivery of  
2 consumers' cellular device usage data, on the "Privacy and Security" page of its website,<sup>2</sup> Carrier  
3 IQ states:

4 Carrier IQ enables mobile operators, mobile device manufacturers,  
5 application vendors and other participants in the Mobile Ecosystem to deliver high  
6 quality products and services, based on what you want, where you want and to work  
7 and perform the way you expect.

8 In providing our products and services, Carrier IQ enables our customers to  
9 gather information on Mobile User Experiences. Carrier IQ's products were  
10 developed from inception to respect and protect user privacy and security. We have  
11 established "Best Practices" approach to privacy and security. Our products are  
12 designed and configured to work within the privacy policies of our end customers  
13 and include functions such as anonymization and encryption. When Carrier IQ's  
14 products are deployed, data gathering is done in a way where the end user is  
15 informed or involved.

16 With deployment on over 130 million phones globally, we have considerable  
17 experience in protecting the privacy of the end user and doing so in a highly secure  
18 manner. Information transmitted from enabled mobile devices is stored in a secure  
19 data center facility that meets or exceeds industry best practice guidelines for  
20 security policies and procedures.

21 Our data gathering and data storage policies are built from industry best  
22 practice. Our products allow us to address privacy & security requirements that vary  
23 country-by-country and customer-by-customer. There are a variety of techniques  
24 involved in protection of privacy and in implementation of security policy,  
25 including anonymization of certain user-identifiable data, aggregation of data and  
26 encryption of data, etc.

27 We work in partnership with our customers to ensure compliance with their  
28 data collection and protection policies. While much of the data we gather data is  
already available through alternate methods, we make it more efficient and useful –  
aimed at improving products, services and quality for the end user.

19 20. However, despite CIQ's statement that "[w]hen Carrier IQ's products are deployed,  
20 data gathering is done in a way where the end user is informed or involved[,]" Plaintiffs and  
21 members of the proposed Class were not informed and had no way to know that Carrier IQ's  
22 software was capturing their keystrokes and intercepting, storing, and transmitting their electronic  
23 communications.

#### 24 **B. Discovery of Carrier IQ's interception of electronic communications**

25 21. In mid-November 2011, a software developer named Trevor Eckhart published on  
26 the web his discovery of the Carrier IQ software on his HTC brand smartphone cellular device.  
27 Mr. Eckhart described the CarrierIQ software as a "rootkit," which is "software that enables

28 <sup>2</sup> [www.carrieriq.com/company/privacy.htm](http://www.carrieriq.com/company/privacy.htm) (last accessed November 30, 2011).

1 continued privileged access to a computer while actively hiding its presence from administrators by  
2 subverting standard operating system functionality or other applications.” (Citing *Wikipedia*.)

3 22. Mr. Eckhart revealed that the CarrierIQ software on his device was virtually  
4 impossible to deactivate, and that it provided no notice that it was embedded and operating and was  
5 capable of logging virtually everything he did on his device, including key strokes, numbers dialed,  
6 SMS (text) messages, and secure (HTTPS) website log-ins and search terms.<sup>3</sup>

7 23. Shortly thereafter, CIQ sent Mr. Eckhart a cease and desist letter demanding in part  
8 that he retract his description of the CIQ software as a rootkit, accusing him of copyright  
9 infringement for posting materials he found on its own website, and threatening severe legal action  
10 if he did not capitulate to its demands. In response, the Electronic Frontier Foundation (“EFF”)  
11 stepped up to Mr. Eckhart’s defense and countered with a letter demonstrating that CIQ’s  
12 accusations were baseless and demanding that CIQ withdraw its letter and threatened legal action.<sup>4</sup>

13 24. On November 23, 2011, CIQ released a statement that provided:

14 As, of today, we are withdrawing our cease and desist letter to Mr. Trevor  
15 Eckhart. We have reached out to Mr. Eckhart and the Electronic Frontier  
16 Foundation (EFF) to apologize. Our action was misguided and we are deeply sorry  
17 for any concern or trouble that our letter may have caused Mr. Eckhart. We  
18 sincerely appreciate and respect EFF’s work on his behalf, and share their  
19 commitment to protecting free speech in a rapidly changing technological world.<sup>5</sup>

20 25. However, the November 23, 2011, CIQ statement also provided:

21 We would like to take this opportunity to reiterate the functionality of  
22 Carrier IQ’s software, what it does not do and what it does:

- 23 - Does not record your keystrokes.
- 24 - Does not provide tracking tools.
- 25 - Does not inspect or report on the content of your communications, such as the  
26 content of emails and SMSs.
- 27 - Does not provide real-time data reporting to any customer.

28 <sup>3</sup> Eckhart’s initial publication can be found at <http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/> (last accessed November 30, 2011).

<sup>4</sup> The letter can be found at: [https://www.eff.org/sites/default/files/eckhart\\_c%26d\\_response.pdf](https://www.eff.org/sites/default/files/eckhart_c%26d_response.pdf)

<sup>5</sup> <http://www.carrieriq.com/company/PR.EckhartStatement.pdf>

1           26. Mr. Eckhart was not convinced by CIQ's denial and performed further analysis on  
2 his active device and an additional device which was no longer subscribed to a cellular service but  
3 was usable over a wi-fi connection.

4           27. On or about November 28, 2011, Mr. Eckhart published his further analysis in a  
5 report titled Carrier IQ Part 2.<sup>6</sup> His report included a 17 minute video in which he stepped through  
6 proof that the CIQ software did, in fact log his key strokes, record his SMS (text) messages, record  
7 dialed numbers, and tracked his internet use, including on HTTPS (secure) websites.

8           28. Mr. Eckhart's report was quickly picked up by the Internet press and broadly  
9 reported. Bryan Chafin, reporting for the *Mac Observer*, wrote:

10                   ...the entire point of the application is to collect and send data  
11 to those servers, so it's not a great stretch to believe that every text,  
12 every search, ever button, and any and every other tap you make on  
13 your HTC Android devices, RIM BlackBerry device, and Nokia  
14 smartphones is being logged and sent to Carrier IQ and then shared  
15 with whichever company paid to have the app there in the first  
16 place.<sup>7</sup>

17                   As you can see in the video, Carrier IQ's claim that the  
18 company is not, "recording keystrokes or providing tracking tools" is  
19 completely false.<sup>8</sup>

20           29. Andy Greenberg, reporting for *Forbes*, wrote:

21                   As Eckhart's analysis of the company's training videos and  
22 the debugging logs on his own HTC Evo handset have shown,  
23 Carrier IQ captures every keystroke on a device as well as location  
24 and other data, and potentially makes that data available to Carrier  
25 IQ's customers. The video he's created (below) shows every  
26 keystroke being sent to the highly-obscured application on the phone  
27 before a call, text message, or Internet data packet is ever  
28 communicated beyond the phone. Eckhart has found the application  
on Samsung, HTC, Nokia and RIM devices, and Carrier IQ claims on

23 <sup>6</sup> <http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/carrieriq-part2/>

24 <sup>7</sup> More specifically, affected devices are reported elsewhere on the Internet to include the Samsung  
25 Epic 4Q, as carried by Sprint; the Samsung Epic 4Q, as carried by Sprint; the Samsung Moment, as  
26 carried by Sprint; the Samsung Infuse, as carried by AT&T; and the Samsung Skyrocket, as carried  
27 by AT&T. The HTC phones are reported to include the HTC Evo, as carried by Sprint and  
28 referenced herein, as well as the Evo 3D, as carried by Sprint. Research is ongoing to determine  
other affected devices.

<sup>8</sup>

[http://www.macobserver.com/tmo/article/carrier\\_iq\\_collects\\_everything\\_on\\_android\\_rim\\_nokia\\_phones/](http://www.macobserver.com/tmo/article/carrier_iq_collects_everything_on_android_rim_nokia_phones/)



1 its website that it has installed the program on more than 140 million  
2 handsets.<sup>9</sup>

3 30. Mr. Greenberg, in the *Forbes* article, went on to quote Carrier IQ as recently stating

4 in part:

5 The information gathered by Carrier IQ is done so for the exclusive  
6 use of that customer, and Carrier IQ does not sell personal subscriber  
7 information to 3rd parties. The information derived from devices is  
8 encrypted and secured within our customer's network or in our  
9 audited and customer-approved facilities.

10 31. Russell Holly, reporting for Geek.com, wrote:

11 Eckhart put together a video of him turning on an HTC  
12 Evo3D with a completely stock (provided by HTC) ROM. He  
13 demonstrates that nowhere in the startup does any mention of  
14 CarrierIQ. There's nothing indicating that this software exists on the  
15 phone. When the applications are discovered, the ability to shut the  
16 apps down the same way you would any other app in Android has  
17 been circumvented. So, you now have a series of applications that  
18 you have to be extremely knowledgeable to find, and when you do  
19 find them they *cannot be turned off*. This is demonstrated in the first  
20 five minutes of the video, and these steps can be easily re-created if  
21 you have access to LogCat on your computer.

22 When you receive a text, the video demonstrates that the  
23 CarrierIQ software is aware of the text message and its contents  
24 before the phone notifies you that you have a message. CarrierIQ and  
25 Sprint both were adamant that the body of an SMS was not recorded,  
26 and yet we can clearly see in the video that the text contents are read  
27 and transmitted via the CarrierIQ applications. In an attempt to clear  
28 this matter up, I reached out to CarrierIQ again, who refused to  
comment and noted that they "are looking forwarding to our meeting  
with EFF this week and will continue to keep you updated."

The video also demonstrates how this software records the  
keys that are pressed in the dialer, before a call is even made.  
Anytime you press a key in the dialer app, even if you just press  
random numbers and then close the application, that information is  
logged by CarrierIQ. If you place a call, that information is recorded  
as well, along with network strength values. This way if anything  
happens that would interrupt the call, your carrier can see why it  
happened and fix it. There's a real benefit to the CarrierIQ software,  
but it is clear that far more is being recorded than is necessary.

....

This video has demonstrated a truly significant volume of  
information is being recorded. Passwords over HTTPS, the contents  
of your text messages, and plenty more are recorded and sent to the  
customers of CarrierIQ. A significant part of what was demonstrated  
is not included in any privacy agreement, and some of it was a direct

<sup>9</sup> <http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases/>

1 contradiction of the statements that were made by these companies. It  
2 looks like we're being lied to, our information is being recorded, and  
3 there is nothing we can do about it.<sup>10</sup>

4 32. Another Android developer, Tim Schofield, extensively researched the presence of  
5 the CIQ software on multiple Android smartphone platforms. He noted that in addition to the  
6 privacy issues, the embedded CIQ software necessarily degrades the performance of any device on  
7 which it is installed. The CIQ software is *always operating and cannot be turned off*. It  
8 necessarily uses system resources, thus slowing performance and decreasing battery life. As a  
9 result, because of the CIQ software, in addition to having their private communications intercepted,  
10 Plaintiffs and Class members are not getting the optimal performance of the smartphone devices  
11 that they purchased, and which are marketed, in part, based on their speed, performance, and  
12 battery life.

13 33. Another harm suffered by Plaintiffs and the Class is that devices running CIQ  
14 embedded software are more vulnerable to data theft than those not running the software. CIQ  
15 software, whether it is transmitting data or not, is capable of intercepting keystrokes and incoming  
16 and outgoing communications. As a result, devices embedded with the CIQ software are  
17 vulnerable to malware, which could piggyback on the CIQ platform to intercept or capture users'  
18 private information and communications.

19 34. Eckhart's test showed his keystrokes being logged and messages intercepted even  
20 when his device was only connected via wi-fi to the Internet. There is no reasonable basis for a  
21 device metric application, which is what Carrier IQ calls its software, to monitor and track device  
22 actions when the device is not connected to a mobile network. This also creates a vulnerability to  
23 data theft and interception via malware transmitted or accessed through wireless connections.

24 **C. Plaintiffs' Cellular Devices Were Embedded With Carrier IQ Software and Their  
25 Communications Were Intercepted Without Authorization**

26 35. Plaintiff Eric Thomas owns and uses a Samsung Replenish smartphone operating on  
27 the Sprint mobile network. This device is embedded with the CIQ software. Plaintiff regularly  
28 sent and received SMS (text) messages on his Samsung device. By virtue of the unknown, not

---

<sup>10</sup> <http://www.geek.com/articles/mobile/security-researcher-responds-to-carrieriq-with-video-proof-20111129/>

1 assented-to, automatic, and unpreventable functions of the CIQ software, Plaintiff's private and  
2 personal communications have been illegally intercepted and transmitted by and to Defendants  
3 Carrier IQ and Samsung. In addition, Plaintiff has not been able to use his smartphone device at  
4 the performance levels it is capable of because the CIQ software is always operating in the  
5 background.

6 36. Plaintiff Benjamin Lancaster owns and uses a Samsung Galaxy S2 Skyrocket  
7 smartphone operating on the AT&T mobile network. This device is embedded with the CIQ  
8 software. Plaintiff regularly sent and received SMS (text) messages on his Samsung device. By  
9 virtue of the unknown, not assented-to, automatic, and unpreventable functions of the CIQ  
10 software, Plaintiff's private and personal communications have been illegally intercepted and  
11 transmitted by and to Defendants Carrier IQ and Samsung. In addition, Plaintiff has not been able  
12 to use his smartphone device at the performance levels it is capable of because the CIQ software is  
13 always operating in the background.

#### 14 V. CLASS ALLEGATIONS

15 37. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure, on  
16 behalf of themselves and a proposed Class consisting of:

17 All persons in the United States that own or owned Samsung brand telephones or  
18 other devices on which Cellular IQ software was installed or embedded.

19 Excluded from the proposed Class are Defendants; Defendants' affiliates and subsidiaries;  
20 Defendants' current or former employees, officers, directors, agents, and representatives; and the  
21 judge or magistrate judge to whom this case is assigned, as well as those judges' immediate family  
22 members.

23 38. **Numerosity:** The exact number of the members of the proposed class is unknown  
24 and is not available to the Plaintiffs at this time, but individual joinder in this case is impracticable.  
25 Based on Defendant CIQ's representation that its software is installed on over 140 million devices,  
26 it is likely that the proposed class consists of tens or hundreds of thousands, or even millions, of  
27 members.  
28

1           39.     **Commonality:** Numerous questions of law and fact are common to the claims of  
2 the Plaintiffs and members of the proposed class. These include:

3           a.     Whether CIQ software installed on Plaintiffs' and proposed class members'  
4 communication devices has intercepted, and whether it has re-transmitted, Plaintiffs' and proposed  
5 Class members' SMS text messages, keystrokes, telephone numbers, and other information, all  
6 without the device owners' knowledge or consent, and whether it continues to do so.

7           b.     Whether CIQ and the Device Manufacturers have violated the Federal Wiretap Act,  
8 18 U.S.C. § 2510 *et seq.*, including the prohibition on the interception, disclosure, and use of wire,  
9 oral, or electronic communications, or otherwise, by way of the acts and omissions set forth in this  
10 complaint.

11          c.     Whether CIQ and the Device Manufacturers have violated the California Unfair  
12 Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* by way of the acts and omissions set  
13 forth in this complaint.

14          d.     Whether CIQ and the Device Manufacturers have unlawfully profited from their  
15 conduct, and whether they must disgorge profits to the Plaintiffs and members of the proposed  
16 Class.

17          e.     Whether Plaintiffs and members of the proposed Class are entitled to statutory and  
18 other damages, civil penalties, punitive damages, restitution, and/or declaratory or injunctive relief.

19          40.     **Typicality:** Plaintiffs' claims are typical of the claims of the members of the  
20 proposed Class. The factual and legal bases of Defendants' liability to Plaintiffs and other  
21 members of the proposed Class are the same and resulted in injury to Plaintiffs and all of the other  
22 members of the proposed Class.

23          41.     **Adequate representation:** Plaintiffs will represent and protect the interests of the  
24 proposed Class both fairly and adequately. They have retained counsel competent and experienced  
25 in complex class-action litigation. Plaintiffs have no interests that are antagonistic to those of the  
26 proposed Class, and their interests do not conflict with the interests of the proposed Class members  
27 they seek to represent.





1           55. Defendants engaged in “fraudulent” business practices under the UCL because they  
2 secretly installed the CIQ software on Plaintiffs’ devices, failed to disclose that the CIQ software  
3 was always operating on such devices, failed to disclose that the CIQ software was capable of  
4 intercepting Plaintiffs’ private communications and, in fact intercepted such communications, and  
5 failed to disclosed that the CIQ software degraded the performance and battery life of the devices  
6 on which it was installed. Defendants’ omissions and failures to disclose were “material” to  
7 Plaintiff and the class within the meaning of *In re Tobacco II Cases* 46 Cal. 4<sup>th</sup> 298, 325 (Cal.  
8 2009).

9           56. Defendant engaged in “unfair” business practices under the UCL based on the  
10 foregoing, and because they violated the laws and underlying legislative policies designed to  
11 protect the privacy rights of Californians and the rights of others which are affected by companies  
12 operating out of California. In particular, Cal. Bus. & Prof. Code §§ 22947-22947.6 and the  
13 California Constitution, which provides:

14                           **ARTICLE 1 DECLARATION OF RIGHTS**

15                           SECTION 1. All people are by nature free and independent and have  
16 inalienable rights. Among these are enjoying and defending life and  
17 liberty, acquiring, possessing, and protecting property, and pursuing  
18 and obtaining safety, happiness, *and privacy*.

19           57. Plaintiff and the Class were injured in fact and lost money or property as a result of  
20 these unlawful, unfair, and fraudulent business practices. In particular and without limitation,  
21 Plaintiffs did not get the performance level and battery life on their phones that they paid for  
22 because the CIQ software necessarily degraded such performance and battery life by constantly  
23 running on Plaintiffs’ devices.

24   **VII. PRAYER FOR RELIEF**

25                           WHEREFORE, Plaintiffs respectfully request the following relief:

26           A. That the Court certify this case as a class action and appoint the named Plaintiffs to  
27 be Class representatives and their counsel to be Class counsel;  
28

1 B. That the Court award them appropriate relief, to include statutory damages, as  
2 available to them under the Federal Wiretap Act, including as that set forth and described in 18  
3 U.S.C. § 2520(b)-(c);

4 C. That the Court award them preliminary or other equitable or declaratory relief as  
5 may be appropriate, per 18 U.S.C. § 2520(b), or by way of other applicable state or federal law;

6 D. Such additional orders or judgments as may be necessary to prevent these practices  
7 and to restore to any person in interest any money or property which may have been acquired by  
8 means of the UCL violations; and

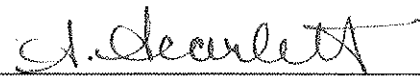
9 E. That the Court award them such other, favorable relief as may be available and  
10 appropriate under federal or state law, or at equity.

11 **VIII. JURY TRIAL DEMANDED**

12 Plaintiffs demand a trial by jury on all issues so triable.

13 DATED: December 2, 2011

14 HAGENS BERMAN SOBOL SHAPIRO LLP

15 By 

16 SHANA E. SCARLETT (217895)

17 715 Hearst Avenue, Suite 202

18 Berkeley, CA 94710

19 Telephone: (510) 725-3000

20 Facsimile: (510) 725-3001

21 shanas@hbsslaw.com

22 Steve W. Berman, *pro hac vice* (application pending)

23 Robert F. Lopez, *pro hac vice* (application pending)

24 Thomas E. Loeser (202724)

25 HAGENS BERMAN SOBOL SHAPIRO LLP

26 1918 Eighth Avenue, Suite 3300

27 Seattle, WA 98101

28 (206) 623-7292

*Attorneys for Plaintiffs and the Proposed Class*