

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

STEVE W. BERMAN, (*pro hac vice* pending)
ROBERT F. LOPEZ, (*pro hac vice* 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@hbsslw.com
robl@hbsslw.com
toml@hbsslw.com

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@hbsslw.com
Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ADR

FILED
DEC - 1 2011
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND

Handwritten notes and signatures, including "Filed" and "12/1/11".

RECEIVED
FAXED

PATRICK KENNY, an Arizona resident,
JUSTIN SHARP, a California resident,
JEREMY FEITELSON, an Iowa resident, and
GREG FEITELSON, a Kentucky resident,
on behalf of themselves and all others similarly
situated,

Plaintiffs,

v.

CARRIER IQ, INC., a Delaware corporation;
HTC CORPORATION, a Taiwanese company;
HTC AMERICA, INC., a Washington
corporation; and SAMSUNG ELECTRONICS
CO., LTD., a Korean company,

Defendants.

No.

C11-05774

CLASS ACTION COMPLAINT

- VIOLATION OF FEDERAL WIRETAP ACT AS AMENDED BY THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510 *et seq.*
- 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..... 10

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.*)..... 13

VII. PRAYER FOR RELIEF..... 14

VIII. JURY TRIAL DEMANDED 15

I. INTRODUCTION

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

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

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

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

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

II. JURISDICTION

22
23 6. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 in
24 that Plaintiffs allege violations of federal law, namely the Federal Wiretap Act as amended by the
25 Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* The Court has supplemental
26 jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a).
27
28

1 7. This Court has personal jurisdiction over the Defendants in this action by way of the
2 fact that Defendants are licensed to do business in the state of California or otherwise conduct
3 business in the state of California.

4 8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) inasmuch as unlawful
5 practices are alleged to have been committed in this federal judicial district and Defendants reside
6 or regularly conduct business in this district.

7 9. Intradistrict assignment: assignment to the San Jose division of this Court is
8 appropriate because Defendant CIQ is a California corporation that has its headquarters in
9 Mountain View, Santa Clara, California, which is located in this division of the Northern District
10 of California. Also, it is believed and therefore alleged that many members of the proposed class
11 reside or do business in the San Jose division of the Northern District of California as well.

12 III. PARTIES

13 10. Plaintiff Patrick Kenny resides in Cave Creek, Arizona.

14 11. Plaintiff Justin Sharp resides in San Francisco, California.

15 12. Plaintiff Jeremy Feitelson resides in West Des Moines, Iowa.

16 13. Plaintiff Greg Feitelson resides in Louisville, Kentucky.

17 14. Defendant Carrier IQ, Inc. is a Delaware corporation, headquartered in Mountain
18 View, California, with additional offices in Chicago, Boston, London (UK) and Kuala Lumpur
19 (Malaysia). On its website, CIQ has a running tally of the number of devices on which its software
20 has been deployed which, as of November 30, 2011, indicated over 141 million cellular devices.

21 15. Defendant HTC Corporation ("HTC") is a Taiwan corporation and cellular device
22 manufacturer located in Taoyuan, Taiwan. HTC has offices within the United States and sells its
23 products throughout the United States, including throughout California. It also is the parent to
24 Defendant HTC America, Inc.

25 16. HTC America, Inc. ("HTC America") is a Washington corporation with its principal
26 place of business in Bellevue, Washington. HTC America sells its products throughout the United
27 States, including throughout California.
28

1 17. Defendant Samsung Electronics Co., Ltd. ("Samsung") is a Korean company with
2 its principal place of business at 1320-10, Seocho 2-dong, Seocho-gu, Seoul 137-857, South Korea.
3 Samsung has offices within the United States and California and sells its products throughout the
4 United States, including throughout California.

5 IV. FACTUAL BACKGROUND

6 A. Carrier IQ

7 18. On its website¹ under the heading, "Who we are," Carrier IQ states:

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

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

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

26 The Carrier IQ solution goes beyond traditional point offerings that address
27 a single business problem, to provide a comprehensive Mobile Service Intelligence
28 platform which builds upon underlying customer experience data to enable all areas
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.

28 ¹ www.carrieriq.com/company/index.htm (last accessed November 30, 2011).

1 20. 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,² 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.

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

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

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

38 ² 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 23. 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.³

7 24. 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.⁴

13 25. 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.⁵

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

⁴ The letter can be found at: https://www.eff.org/sites/default/files/eckhart_c%26d_response.pdf

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

1 27. 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 28. On or about November 28, 2011, Mr. Eckhart published his further analysis in a
5 report titled Carrier IQ Part 2.⁶ 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 29. 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.⁷

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.⁸

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

24 ⁷ 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.

29 ⁸
30 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.⁹

3 31. 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 32. 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

⁹ <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.¹⁰

4 33. 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 **C. Plaintiffs' Cellular Devices Were Embedded With Carrier IQ Software and Their**
14 **Communications Were Intercepted Without Authorization**

15 34. Plaintiff Patrick Kenny currently (and for the past several months) has owned and
16 used a Samsung Galaxy smartphone operating on the Sprint mobile network. This device is
17 imbedded with the CIQ software. Plaintiff regularly sends and receives SMS (text) messages on
18 his Samsung device. By virtue of the unknown, not assented-to, automatic, and unpreventable
19 functions of the CIQ software, Plaintiff's private and personal communications have been illegally
20 intercepted and transmitted by and to Defendants Carrier IQ and Samsung. In addition, Plaintiff
21 has not been able to use his smartphone device at the performance levels it is capable of because
22 the CIQ software is always operating in the background.

23 35. Plaintiff Patrick Kenny previously owned and used an HTC Touch smartphone
24 operating on the Sprint mobile network. This device is imbedded with the CIQ software. Plaintiff
25 regularly sent and received SMS (text) messages on his HTC device. By virtue of the unknown,
26 not assented-to, automatic, and unpreventable functions of the CIQ software, Plaintiff's private and
27 personal communications have been illegally intercepted and transmitted by and to Defendants
28 Carrier IQ and HTC and/or HTC America. In addition, Plaintiff has not been able to use his

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

1 smartphone device at the performance levels it is capable of because the CIQ software is always
2 operating in the background.

3 36. Plaintiff Justin Sharp owns and uses an HTC Evo 4 smartphone operating on the
4 Sprint mobile network. This device is imbedded with the CIQ software. Plaintiff regularly sent
5 and received SMS (text) messages on his HTC device. By virtue of the unknown, not assented-to,
6 automatic, and unpreventable functions of the CIQ software, Plaintiff's private and personal
7 communications have been illegally intercepted and transmitted by and to Defendants Carrier IQ
8 and HTC and/or HTC America. In addition, Plaintiff has not been able to use his smartphone
9 device at the performance levels it is capable of because the CIQ software is always operating in
10 the background.

11 37. Plaintiff Jeremy Feitelson owns and uses an HTC Evo smartphone operating on the
12 Sprint mobile network. This device is imbedded with the CIQ software. Plaintiff regularly sent
13 and received SMS (text) messages on his HTC device. By virtue of the unknown, not assented-to,
14 automatic, and unpreventable functions of the CIQ software, Plaintiff's private and personal
15 communications have been illegally intercepted and transmitted by and to Defendants Carrier IQ
16 and HTC and/or HTC America. In addition, Plaintiff has not been able to use his smartphone
17 device at the performance levels it is capable of because the CIQ software is always operating in
18 the background.

19 38. Plaintiff Greg Feitelson owns and uses an HTC Evo 3D smartphone operating on
20 the Sprint mobile network. This device is imbedded with the CIQ software. Plaintiff regularly sent
21 and received SMS (text) messages on his HTC device. By virtue of the unknown, not assented-to,
22 automatic, and unpreventable functions of the CIQ software, Plaintiff's private and personal
23 communications have been illegally intercepted and transmitted by and to Defendants Carrier IQ
24 and HTC and/or HTC America. In addition, Plaintiff has not been able to use his smartphone
25 device at the performance levels it is capable of because the CIQ software is always operating in
26 the background.

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

V. CLASS ALLEGATIONS

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

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

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

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

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

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

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

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

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

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

6 42. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the
7 proposed Class. The factual and legal bases of Defendants' liability to Plaintiffs and other
8 members of the proposed Class are the same and resulted in injury to Plaintiffs and all of the other
9 members of the proposed Class.

10 43. **Adequate representation:** Plaintiffs will represent and protect the interests of the
11 proposed Class both fairly and adequately. They have retained counsel competent and experienced
12 in complex class-action litigation. Plaintiffs have no interests that are antagonistic to those of the
13 proposed Class, and their interests do not conflict with the interests of the proposed Class members
14 they seek to represent.

15 44. **Predominance and Superiority:** This proposed class action is appropriate for
16 certification. Class proceedings on these facts and this law are superior to all other available
17 methods for the fair and efficient adjudication of this controversy, given that joinder of all
18 members is impracticable. Even if members of the proposed Class could sustain individual
19 litigation, that course would not be preferable to a class action because individual litigation would
20 increase the delay and expense to all parties due to the complex factual and legal controversies
21 present in this controversy. Here, the class action device will present far fewer management
22 difficulties, and it will provide the benefit of a single adjudication, economies of scale, and
23 comprehensive supervision by this Court. Further, uniformity of decisions will be ensured.

24 VI. CLAIMS FOR RELIEF

25 COUNT I 26 VIOLATION OF THE FEDERAL WIRETAP ACT

27 45. Plaintiffs repeat and re-allege every allegation above as if set forth herein in full.
28

1 46. Plaintiffs bring this claim on their own behalf and on behalf of each member of the
2 proposed Class described above

3 47. Defendants Carrier IQ and the Device Manufacturers, by way of the Carrier IQ
4 software and their own implementing or ancillary software, have intentionally intercepted,
5 endeavored to intercept, or procured others to intercept or endeavor to intercept, wire and/or
6 electronic communications as described herein, all without the knowledge, consent or authorization
7 of Plaintiffs or the Class, in violation of 18 U.S.C. § 2511(1). *See* 18 U.S.C. § 2511(1)(a).

8 48. Defendants Carrier IQ and the Device Manufacturers, by way of the Carrier IQ
9 software and their own implementing or ancillary software, have intentionally disclosed, or
10 endeavored to disclose, to other persons the contents of wire and/or electronic communications,
11 knowing or having reason to know that the information was obtained through the interception of
12 wire or electronic communications, as described in 18 U.S.C. § 2511(1)(c). Accordingly, these
13 Defendants have violated 18 U.S.C. § 2511(1).

14 49. As a result of these violations of law, Plaintiffs and the class and suffered harm and
15 injury, including the interception and transmission of private and personal communications and the
16 degraded performance level of the devices in question.

17 50. As a result of these violations of law, Defendants Carrier IQ and the Device
18 Manufacturers are subject to civil suit, and Plaintiffs are entitled to appropriate relief, including
19 that set forth in 18 U.S.C. § 2520(b). 18 U.S.C. § 2520(a). Such appropriate relief includes
20 “preliminary or other equitable or declaratory relief as may be appropriate”; “damages” as
21 described in the statute; and “a reasonable attorney’s fee and other litigation costs reasonably
22 incurred.” 18 U.S.C. § 2520(b). As for damages, “the court may assess as damages whichever is
23 the greater of—(A) the sum of the actual damages suffered by the Plaintiff and any profits made by
24 the violator as a result of the violation; or (B) statutory damages of whichever is the greater of \$100
25 a day for each day of violation or \$10,000.” 18 U.S.C. § 2520(c)(2).

26 51. Plaintiffs, on their own behalf and on behalf of the proposed Class, seek all such
27 appropriate relief, including but not limited to statutory damages as set forth above.
28

COUNT II
VIOLATION OF THE UNFAIR COMPETITION LAW
(CAL. BUS. & PROF. CODE §§ 17200 ET SEQ.)

52. Plaintiffs repeat and re-allege every allegation above as if set forth herein in full.

53. Plaintiffs bring this claim on their own behalf and on behalf of each member of the proposed Class described above.

54. California's Unfair Competition Law (the "UCL") defines unfair competition to include any "unlawful, unfair, or fraudulent" business act or practice. Cal. Bus. & Prof. Code §§ 17200 *et seq.*

55. Defendants engaged in "unlawful" business practices under the UCL because they violated the Federal Wiretap Act, 18 U.S.C. § 2511.

56. Defendants engaged in "unlawful" business practices under the UCL because they violated the California Consumer Protection Against Spyware Act, Cal. Bus. & Prof. Code §§ 22947-22947.6.

57. Defendants engaged in "fraudulent" business practices under the UCL because they secretly installed the CIQ software on Plaintiffs' devices, failed to disclose that the CIQ software was always operating on such devices, failed to disclose that the CIQ software was capable of intercepting Plaintiffs' private communications and, in fact intercepted such communications, and failed to disclose that the CIQ software degraded the performance and battery life of the devices on which it was installed. Defendants' omissions and failures to disclose were "material" to Plaintiff and the class within the meaning of *In re Tobacco II Cases* 46 Cal. 4th 298, 325 (Cal. 2009).

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

ARTICLE 1 DECLARATION OF RIGHTS

SECTION 1. All people are by nature free and independent and have

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


VIII. JURY TRIAL DEMANDED

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

DATED: December 1, 2011

HAGENS BERMAN SOBOL SHAPIRO LLP

STEVE W. BERMAN, (*pro hac vice* pending)
ROBERT F. LOPEZ, (*pro hac vice* pending)
THOMAS E. LOESER (202724)
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

By 
SHANA E. SCARLETT

HAGENS BERMAN SOBOL SHAPIRO LLP
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Telephone: (510) 725-3000
Facsimile: (510) 725-3001
shanas@hbsslaw.com
Attorneys for Plaintiffs and the Proposed Class