

FILED
2011 DEC -2 P 2:55
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
N.D. CA. - SAN JOSE
Leis
Paul
S

1 CLIFFORD H. PEARSON (Bar No. 108523)
cpearson@pswplaw.com
2 DANIEL L. WARSHAW (Bar No. 185365)
dwarshaw@pswplaw.com
3 BOBBY POUYA (Bar No. 245527)
bpouya@pswplaw.com
4 **PEARSON, SIMON, WARSHAW & PENNY, LLP**
15165 Ventura Boulevard, Suite 400
5 Sherman Oaks, California 91403
Telephone: (818) 788-8300
6 Facsimile: (818) 788-8104

7 BRUCE L. SIMON (Bar No. 96241)
bsimon@pswplaw.com
8 AARON M. SHEANIN (Bar No. 214472)
asheanin@pswplaw.com
9 THOMAS K. BOARDMAN (Bar No. 276313)
tboardman@pswplaw.com

10 **PEARSON, SIMON, WARSHAW & PENNY, LLP**
44 Montgomery Street, Suite 2450
11 San Francisco, California 94104
Telephone: (415) 433 9000
12 Facsimile: (415) 433 9008

13 Attorneys for Plaintiffs Daniel Pipkin and Chad Ulrich,
on Behalf of Themselves and All Others Similarly
14 Situated

15 **UNITED STATES DISTRICT COURT**
16 **NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION**

HRL

18 DANIEL PIPKIN and CHAD ULRICH, on
Behalf of Themselves and All Others Similarly
19 Situated,

20 Plaintiffs,

21 vs.

22 CARRIER IQ, INC.; SAMSUNG
ELECTRONICS AMERICA, INC.;
23 SAMSUNG TELECOMMUNICATIONS
AMERICA, INC.; HTC AMERICA, INC.

24 Defendants.
25
26
27
28

CV 11-05820
CASE NO.

CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL

PEARSON, SIMON, WARSHAW & PENNY, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

1 Plaintiffs Daniel Pipkin and Chad Ulrich (“Plaintiffs”), on behalf of themselves and all
2 others similarly situated, allege the following on information and belief:

3 **I. INTRODUCTION**

4 1. This class action lawsuit arises out of the undisclosed and unauthorized monitoring
5 and recording of the keystrokes, data sent and received, location, habits, numbers dialed, message
6 content, websites visited, web searches, and other private information of millions of mobile device
7 users by Defendant Carrier IQ, Inc. (“Carrier IQ”) and its partner mobile device manufacturers
8 including, but not limited to, Defendants Samsung Electronics America, Inc., Samsung
9 Telecommunications America, Inc. (“Samsung”), and HTC America, Inc. (“HTC”) (collectively
10 “Defendants”).

11 2. During the Class Period, Carrier IQ designed and distributed performance
12 monitoring software (“Carrier IQ Software”), which was installed on hundreds of millions of
13 mobile phones, smartphones, and other mobile devices by leading mobile device manufacturers
14 including, but not limited to, Samsung and HTC. The Carrier IQ Software is preinstalled on these
15 mobile devices and is designed to automatically secretly track and record information regarding
16 the use and operation of these mobile devices without obtaining user consent or authorization.

17 3. Unbeknownst to mobile device users, the Carrier IQ Software tracks, stores, and
18 records extremely private user information from their mobile devices. Furthermore, the Carrier IQ
19 Software cannot be uninstalled, turned off, or otherwise deactivated, even when discovered. As
20 such, the only way mobile device users can prevent their private information from being accessed
21 is to completely cease the use and operation of their mobile devices.

22 4. Plaintiffs bring this lawsuit on behalf of all similarly situated operators of mobile
23 phone devices and allege that Defendants’ conduct constitutes an unlawful violation of the Federal
24 Wiretap Act (18 U.S.C. §§ 2511, *et seq.*) and the Computer Fraud and Abuse Act (18 U.S.C.
25 §§ 1030, *et seq.*). Plaintiffs further allege that Defendants have violated the rights of California
26 residents by engaging in unlawful wiretapping in violation of California Penal Code § 631 and
27 recording cellular communications without consent in violation of California Penal Code § 637.2.
28

1
2 **II. PARTIES**

3 **PLAINTIFFS:**

4 5. Plaintiff Daniel Pipkin is an individual residing in Ventura County, California. Mr.
5 Pipkin purchased and operated a Samsung Galaxy S2 4G LTE mobile device. Mr. Pipkin did not
6 know that his mobile device was equipped with the Carrier IQ Software and recording private
7 information regarding the use and operation of his mobile device. Mr. Pipkin did not authorize
8 Samsung or Carrier IQ to utilize the Carrier IQ Software on his mobile device or to otherwise
9 disclose his private information utilizing the Carrier IQ Software.

10 6. Plaintiff Chad Ulrich is an individual residing in Ventura County, California. Mr.
11 Ulrich purchased and operated an HTC Droid Incredible mobile device. Mr. Ulrich did not know
12 that his mobile device was equipped with the Carrier IQ Software and recording private
13 information regarding the use and operation of his mobile device. Mr. Ulrich did not authorize
14 HTC or Carrier IQ to utilize the Carrier IQ Software on his mobile device or to otherwise disclose
15 his private information utilizing the Carrier IQ Software.

16 **DEFENDANTS:**

17 7. Defendant Carrier IQ, Inc. is a Delaware corporation with its principal place of
18 business, corporate headquarters, and agent for service of process located at 1200 Villa Street,
19 Suite 200, Mountain View, CA 94041. At all relevant times alleged herein, Carrier IQ made its
20 business decisions from its corporate headquarters in Mountain View, California.

21 8. Defendant Samsung Electronics America, Inc. is a New York corporation with its
22 principal place of business located at 105 Challenger Road, Ridgefield Park, New Jersey 07660.

23 9. Defendant Samsung Telecommunications America, Inc. is a Delaware corporation
24 with its principal place of business located at 1301 East Lookout Drive, Richardson, Texas 75081.

25 10. Defendant HTC America, Inc. is a Washington corporation with its principal place
26 of business located at 811 1st Ave., Suite 530, Seattle, Washington 98104.

27 11. At all times mentioned herein, Defendants, and each of them, were members of,
28 and engaged in, a joint venture, partnership, and common enterprise, and acted within the course
and scope of, and in pursuance of, said joint venture, partnership, and common enterprise.

1 12. At all times mentioned herein, the acts and omissions of Defendants, and each of
2 them, contributed to the various acts and omissions of each and all of the other Defendants in
3 proximately causing the injuries and damages as alleged herein.

4 13. At all times mentioned herein, Defendants, and each of them, ratified each and
5 every act or omission complained of herein. At all times mentioned herein, Defendants, and each
6 of them, aided and abetted the acts and omissions of each and all of the other Defendants in
7 proximately causing the damages as alleged herein.

8 III. JURISDICTION AND VENUE

9 14. Pursuant to 28 U.S.C. § 1331, this Court has original jurisdiction over this lawsuit
10 arising under the Electronic Communications Privacy Act (18 U.S.C. §§ 2511 *et seq.*) and the
11 Computer Fraud and Abuse Act (18 U.S.C. §§ 1030, *et seq.*).

12 15. The Court further has jurisdiction over Plaintiffs' claims brought under California
13 law pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005
14 ("CAFA"), Pub. L. No. 109-2, 119 Stat. 4 (2005), which explicitly provides for the original
15 jurisdiction of the Federal Courts of any class action in which any member of the class is a citizen
16 of a state different from any defendant, and in which the matter in controversy exceeds in the
17 aggregate the sum of \$5,000,000.00, exclusive of interest and costs.

18 16. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(a) and (c)
19 because Defendant Carrier IQ resides in the district, a substantial part of the events or omissions
20 giving rise to the claims occurred in this district, and the parties have contracted to adjudicate their
21 disputes in this district.

22 IV. FACTUAL ALLEGATIONS

23 **A. Background on Carrier IQ and its Mobile Performance Monitoring Software**

24 17. Carrier IQ is a manufacturer of mobile performance monitoring software and
25 describes itself as "the world's leading provider of Mobile Service Intelligence solutions."¹

26
27 ¹ <http://www.carrieriq.com/company/index.htm> (last viewed on December 1, 2011).
28

1 Carrier IQ designs its mobile performance monitoring software in order to obtain information
2 regarding the manner that consumers utilize their mobile devices.

3 18. Carrier IQ describes its goals and services on its website as follows:

4 Our mission is to provide mobile carriers and device OEMs with
5 *unprecedented insight into service performance and usability* and
6 so enable them to deliver higher quality products and services to
7 their customers.

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

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

22 Recognizing the phone as an integral part of a mobile service
23 delivery, and using the device to measure key parameters of service
24 quality and usage, *the Carrier IQ solution gives you the unique*
25 *ability to analyze in detail usage scenarios and fault conditions by*
26 *type, location, application and network performance while*
27 *providing you with a detailed insight into the mobile experience as*
28 *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.²

19. According to Carrier IQ, its software is currently deployed on over 140,000,000
handsets throughout the world and counting.³

² *Id.* (emphasis added).

³ <http://www.carrieriq.com>.

B. The Carrier IQ Software Records Private User Information, Including User Location, Keystrokes, Message Content, and Data Without Disclosure

20. In order to obtain and record this “unprecedented insight into the service and performance from end users,” Carrier IQ’s Software is preinstalled on mobile devices, including mobile phones and smartphones manufactured by Samsung and HTC. The Carrier IQ Software can only be installed on these mobile devices with the express knowledge and permission of Samsung, HTC, and other mobile device manufacturers.

21. The Carrier IQ Software is a “rootkit,” meaning it runs in the background of the mobile device and hides itself from the user while enabling privileged access to the user’s data. The Carrier IQ Software runs on the mobile device without user authorization as soon as the device is enabled. Defendants do not provide consumers with privacy disclosures or otherwise provide consumers with the opportunity to disclose their private information before the software starts running or anytime thereafter. Indeed, the Carrier IQ Software is specifically designed in a manner that does not allow mobile device users to discover the operation or existence of the Carrier IQ Software.

22. Even if a mobile device user is savvy enough to discover the existence of the Carrier IQ Software, the Carrier IQ Software cannot be uninstalled, deactivated, or otherwise removed from the mobile device. As such, the only way users of mobile devices containing Carrier IQ Software can prevent the private information is to completely cease the use of their mobile device.

23. Once the Carrier IQ Software is installed on a mobile device, it exploits this unauthorized access to record and transmit highly private information pertaining to the conduct, communications, and experience of mobile device operators. This recorded activity specifically extends to almost every aspect of the mobile device experience and includes, but is not limited to:

- a. The location of the mobile device operator;
- b. Keystrokes made on the mobile device;
- c. The telephone numbers dialed and received by the mobile device operator;
- d. The contents of text messages sent and received by the mobile device

1 operator;

2 e. The contents of emails sent and received by the mobile device operator; and

3 f. All data transmitted and received through secured and unsecured websites.

4 24. In other words, the Carrier IQ Software records essentially everything the mobile
5 device operator does on the mobile device without authorization or disclosure and constitutes a
6 shocking breach of privacy and confidentiality.

7 **C. Carrier IQ's Unauthorized Collection of Private Information is Exposed by a**
8 **Technology Blogger**

9 25. Throughout the Class Period, Defendants have purposely concealed the existence,
10 capabilities, and functions of the Carrier IQ Software from consumers. Defendants have
11 accomplished this by designing the Carrier IQ Software so that it cannot be detected by
12 consumers, and refusing to provide consumers with privacy disclosures or other means to consent
13 to the installation and operation of the Carrier IQ Software. Unlike consumer applications, which
14 are purchased by and designed for the benefit and enjoyment of the consumer, the purpose of the
15 Carrier IQ Software is to secretly record operator activity for the benefit of the manufacturer.

16 26. In November 2011, a technology blogger and research developer named Trevor
17 Eckhart disclosed on his blog that Carrier IQ has been tracking user activity without authorization
18 or disclosure. Mr. Eckhart posted a seventeen-minute video on the internet depicting the Carrier
19 IQ Software's step-by-step logging and recording of keystrokes Mr. Eckhart made on his HTC
20 mobile device.⁴

21 27. Rather than modify its practices, Carrier IQ sought to silence Mr. Eckhart by
22 sending him a cease and desist letter on November 16, 2011 and threatening to institute a
23 copyright infringement action against him arising from the unauthorized use of Carrier IQ's
24 training materials. *See* Carrier IQ Cease and Desist Letter, attached as Exhibit "A." Carrier IQ's
25 cease and desist letter stated in relevant part:

26

27 ⁴ *See* http://www.youtube.com/watch?v=T17XQI_AYNo&feature=player_embedded#!

28

1 the consequences of copyright infringement include statutory
2 damages between \$750 and \$30,000 per work, at the discretion of
3 the court, and damages up to \$150,000 per work for willful
4 infringement. If you continue to engage in copyright infringement
5 after receiving this letter, your actions will be evidence of 'willful
6 infringement.'

7 28. Although the letter makes a vague reference to false representations made by Mr.
8 Eckhart, it fails to articulate any basis to take legal action with regard to Mr. Eckhart's exposure of
9 Carrier IQ's unlawful monitoring and recording of mobile device user activity.

10 29. In response to Carrier IQ's letter, Mr. Eckhart enlisted the services of the Electronic
11 Frontier Foundation, a non-profit organization dedicated to defending freedom of speech and
12 expression on the internet. On November 23, 2011, Carrier IQ issued a press release officially
13 withdrawing its cease and desist letter to Mr. Eckhart and publicly apologizing to Mr. Eckhart and
14 the Electronic Frontier Foundation. See Carrier IQ Press Release (Nov. 23, 2011), attached as
15 Exhibit "B."

16 30. Carrier IQ's November 23, 2011 press release went on to deny that the Carrier IQ
17 Software records keystrokes, provides tracking tools, inspects and records the content of
18 communications, or provides real-time data reporting to any customer. Plaintiffs allege that each
19 of the denials in Carrier IQ's November 23, 2011 press release are false, misleading, and
20 fraudulently conceal the true qualities of Carrier IQ Software.

21 **D. Revelation of Carrier IQ's Unlawful Collection of Private Mobile User**
22 **Information Outrages the Public, Industry Commentators, and the United**
23 **States Congress**

24 31. The shocking disclosure of Carrier IQ's unauthorized collection and utilization of
25 private mobile user information has resulted in significant backlash and outrage by consumers and
26 industry commentators, and led to the initiation of an investigation by the United States Senate
27 Judiciary Committee.

28 32. Upon the public disclosure of Carrier IQ's violation of consumer privacy rights,
consumers have reacted with outrage and called for swift legal action to be taken against Carrier
IQ and its manufacturer partners. The following are examples of these complaints:

1 a. "I have to say . . . this is insanity!! If companies were trying
2 to obtain knowledge about "the user's experience-" they wouldnt
3 [sic] need to know every single word that is typed into SMS or the
4 Web, rather just that we are using text messages or the web. They
5 have gone TOO FAR by going into peoples personal data, without
6 concent [sic]! There must be a way to prosecute!-! We as users
7 didnt [sic] AGREE to this , and we should be able to get rid of it! It
8 is a VIOLATION OF PRIVACY and action needs to be taken!"

9 b. "By reporting the private numbers called by an end user,
10 CIQ has not only violated the privacy of the user but of the call
11 recipient. Pretend you are a patient with a socially embarrassing [sic]
12 condition and your doctor calls you on his HTC or Samsung... they
13 know you were called. This is actually a violation of HIPPA. You
14 never signed a consent for disclosure of any medical information. If
15 he or she replied with a text, they now know what your condition is
16 and what treatment has been discussed. Does that make you feel
17 warm and fuzzy? This is a major lawsuit..."

18 c. "All I want is a phone that can be with me for medical
19 emergencies. Why do they have to data mine everything I do
20 without my permission? The most frightening part of this is that they
21 have disabled the security when you go to an https site. Not a
22 problem for me since the phone is just a phone in my useage [sic],
23 but it is serious for those who have bought into using their phone for
24 everything from banking to websurfing to scanning tags in stores for
25 more information on a product."

26 d. "The Carrier I.Q. statement about using the app to get
27 informaton [sic] on how the product works sounds like total crap - to
28 me is [sic] is spying on customers so that the information can be
used in sales of products current and possibly in the future. No one
has a right to know what sites you visit. And I think it is a real
violation of trust to have the app installed and not making
consumers aware of it and what it does, and how to shut the damned
thing off. I don't like anyone tracking my movements because I don't
trust their reasons for doing it will always be legitimate and in my
personal interest."

29 e. "Isn't this wireless tapping in it's most malicious form
30 inasmuch the usuer [sic] is not aware that he is being hacked by
31 Current IQ? Common [sic] people this has to end. We are all sheep
32 being led to the slaughter sublimely and the purpetrators [sic] are
33 reaping \$ millions from our letting them get away with it. It's time to
34 kick these companies off of our phones or have the ability to disable
35 all these wireless tapping programs embedded surrupitiously [sic]
36 on our phones and computers."

37 f. "I'm pretty sure there is some form of legal ramifications
38 involved with this.... this is DEFINITELY an invasion of privacy for
those who did not approve the app on their phones. Super shady
business going on here.

"Why is this not opt-in and why is it so hard to fully remove?" Eckhart wrote at the

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

end of the video.’

Why exactly ---- ? ? ? ? This is creepy.”

g. “Carrier IQ showed *their* colors when the first thing they tried to do was silence the security researcher who uncovered their software by filing a SLAPP lawsuit against him (since withdrawn after a stinging rebuke from the EFF). This company should be prosecuted for violation of US anti-wiretap laws. And carriers should drop them like the poisonous hot potato they are.”

h. “Even without this IQ spyware, mobile phones are effectively tracking devices. But this latest discovery is ten times worse. This has to be highly illegal. Remember how British Telecom at first issues denials that their Phorm product was tracking web users, but then it was judged to be illegal. We need class-action law suits [sic] prosecute the phone manufacturers and the makers of this rootkit.”

33. Technology blogs, magazines, and websites have echoed the sentiments of consumers, arguing that the unauthorized recording of user data by Carrier IQ is unfair and unlawful.

34. An article published in Forbes Magazine entitled “Phone ‘Rootkit’ Maker Carrier IQ May Have Violated Wiretap Law in Millions of Cases,” reads in relevant part as follows:

A piece of keystroke-sniffing software called Carrier IQ has been embedded so deeply in millions of Nokia, Android, and RIM devices that it’s tough to spot and nearly impossible to remove, as 25-year old Connecticut systems administrator Trevor Eckhart revealed in a video Tuesday.

That’s not just creepy, says Paul Ohm, a former Justice Department prosecutor and law professor at the University of Colorado Law School. He thinks it’s also likely grounds for a class action lawsuit based on a federal wiretapping law.

“If Carrier IQ has gotten the handset manufactures to install secret software that records keystrokes intended for text messaging and the Internet and are sending some of that information back somewhere, this is very likely a federal wiretap.” he says. “And that gives the people wiretapped the right to sue and provides for significant monetary damages.”⁵

⁵ See Greenberg, Andy, Phone ‘Rootkit’ Maker Carrier IQ May Have Violated Wiretap Law in Millions of Case, available at <http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases/> (last viewed on Dec. 1, 2011).

1 35. An article published on Blogcritics.com went even further in capturing the
2 emotional reaction of consumers, describing Mr. Eckhart's video as follows:

3 The [Eckhart] video paints a pretty creepy picture about what kind
4 of data this software is able to pick up and I warn you, you may feel
5 a little ill watching it. Eckhart uses a factory-reset, non-rooted HTC
6 Evo (as he says, not to single out HTC but it was just what he had on
7 hand) to show not only how the software is hidden and unable to be
8 shut down, but how it appears to also have a built-in keylogger.
9 Each key press looks like it has its own code, so anyone taking a
10 look can see what letters and numbers are being entered.

11 The killer is that this also covers passwords, browser entries, and
12 even HTTPS browser entries, which is supposed to be encrypted.
13 HTTPS browsing is designed to encrypt data so anyone planning to
14 pick up any data would be thwarted. Oh right, text message and
15 SMS content counts too. Data from messages gets sent off to Carrier
16 IQ's servers without anyone being the wiser. Eckhart classifies this
17 as a rootkit, which is a label I wholeheartedly agree with. It gets
18 into your system, acts with administrator privileges, and you can't
19 get rid of the software unless you void the warranty and do the
20 rooting yourself. But it gets even worse. Even as Eckhart was
21 running in airplane mode (cellular radio off) and on wifi only, the
22 app still logged everything that was going on while "disconnected"
23 from the Sprint network. It's the sort of thing that makes me
24 wonder if all the conspiracy theorists are right and that I should be
25 equipped with a tinfoil hat.⁶

26 36. Carrier IQ's conduct has also caught the ire of the United States Senate Judiciary
27 Committee, which has initiated an investigation into this matter. In a letter dated November 30,
28 2011 to the President and CEO of Carrier IQ, Larry Lenhart, United States Senator Al Franken
wrote:

29 I am very concerned by recent reports that your company's software
30 – pre-installed on smartphones used by millions of Americans – is
31 logging and may be transmitting extraordinarily sensitive
32 information from consumers' phones

33 . . .

34 I understand the need to provide usage and diagnostic information to
35 carriers. I also understand that carriers can modify Carrier IQ's

36 ⁶ See Nene, Tushar, Smartphone Spy - Mobile Carriers Caught Secretly Skimming Android User
37 Info, available at [http://blogcritics.org/scitech/article/smartphone-spy-mobile-carriers-caught-](http://blogcritics.org/scitech/article/smartphone-spy-mobile-carriers-caught-secretly/)
38 secretly/ (last viewed on Dec. 1, 2011).

1 software. But it appears that Carrier IQ's software captures a broad
2 swath of extremely sensitive information from users that would
3 appear to have nothing to do with diagnostics – including who they
4 are calling, the *contents* of the texts they are receiving, the *contents*
5 of their searches, and the websites they visit.

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

9 United State Senate Judiciary Committee Letter to Larry Lenhart (Nov. 30, 2011), attached as
10 Exhibit "C."

11 37. Senator Franken's letter requests that Carrier IQ answer questions regarding the
12 consumer information that it collects and the methods it uses that information no later than
13 December 14, 2011.

14 **V. CLASS ACTION ALLEGATIONS**

15 38. Plaintiffs bring this action on behalf of themselves and all other similarly situated
16 members of the following proposed Subclasses pursuant to Federal Rule of Civil Procedure 23:

17 **Carrier IQ Subclass:**

18 All individuals and entities residing in the United States who operated a
19 mobile device equipped with the Carrier IQ Software.

20 **Samsung Subclass:**

21 All individuals residing in the United States who operated a Samsung
22 mobile device equipped with the Carrier IQ Software.

23 **HTC Subclass:**

24 All individuals residing in the United States who operated an HTC mobile
25 device equipped with the Carrier IQ Software.

26 39. The following persons shall be excluded from the Subclasses: (1) Defendants and
27 their subsidiaries, affiliates, officers, and employees; (2) all persons who make a timely election to
28 be excluded from the proposed Class; (3) governmental entities; and (4) the judge(s) to whom this
case is assigned and any immediate family members thereof.

40. Plaintiffs reserve the right to amend the class definitions prior to class certification.

41. Although the exact number of Class Members is uncertain and can only be

1 ascertained through appropriate discovery, Plaintiffs are informed and reasonably believe the
2 number of Class Members is in the millions, such that joinder is impracticable.

3 42. The Class is composed of an easily ascertainable, self-identifying set of individuals
4 and entities that operated mobile devices equipped with the Carrier IQ Software. The Class can be
5 readily identified through Defendants' records.

6 43. There is a well-defined community of interest among the proposed Class Members,
7 and the disposition of all of their claims in a single action will provide substantial benefits to all
8 parties and to the Court.

9 44. The claims of the representative Plaintiffs are typical of the claims of the Class in
10 that the representative Plaintiffs, like all Class Members, operated mobile devices equipped with
11 the Carrier IQ Software.

12 45. The representative Plaintiffs and all Class Members have been injured in that they
13 have had their privacy rights violated as a result of Defendants' misconduct.

14 46. The factual basis for Defendants' misconduct is common to all Class Members and
15 represents a common thread of wrongdoing resulting in injury to all Class Members.

16 47. Plaintiffs will fairly and adequately protect the interests of the Class. They have
17 retained counsel with substantial experience in prosecuting consumer class actions, and
18 specifically actions involving defective products.

19 48. Plaintiffs and their counsel are committed to prosecuting this action vigorously on
20 behalf of the Class, and have the financial resources to do so. Neither Plaintiffs nor their counsel
21 have any interests adverse to those of the Class.

22 49. Plaintiffs and Class Members have all suffered and will continue to suffer harm and
23 damages as a result of Defendants' unlawful and wrongful conduct.

24 50. The prosecution of separate actions by thousands of individual Class Members
25 would create a risk of inconsistent or varying adjudications with respect to individual Class
26 Members, thus establishing incompatible standards of conduct for Defendants.

27 51. The prosecution of separate actions by individual Class Members would also create
28 the risk of adjudications with respect to them that would, as a practical matter, be dispositive of

1 the interests of the other Class Members who are not a party to such adjudications and would
2 substantially impair or impede the ability of such non-party Class Members to protect their
3 interests.

4 52. Defendants have acted or refused to act on grounds generally applicable to the
5 entire Class, thereby making appropriate final declaratory and injunctive relief with respect to the
6 Class as a whole.

7 53. There are numerous questions of law and fact common to Plaintiffs and the Class
8 that predominate over any questions that may affect individual Class Members, including the
9 following:

10 a. Whether Defendants monitored, intercepted, recorded, and/or stored data
11 and other private information from Plaintiffs' and Class Members' mobile devices;

12 b. Whether Defendants made false and misleading statements regarding the
13 safety and security of the Carrier IQ Software;

14 c. Whether Defendants' conduct violates the Federal Wiretap Act (18 U.S.C.
15 §§ 2511, *et seq.*);

16 d. Whether Defendants' conduct violates the Computer Fraud and Abuse Act
17 (18 U.S.C. §§ 1030, *et seq.*);

18 e. Whether Defendants' conduct violates Section 631 of the California Penal
19 Code;

20 f. Whether Defendants' conduct violates Section 632.7 of the California Penal
21 Code;

22 g. Whether Defendants are liable for statutory damages under Section 637.2 of
23 the California Penal Code;

24 h. Whether Plaintiffs and the Class are entitled to compensatory, exemplary,
25 and statutory damages, and the amount of such damages; and

26 i. Whether Carrier IQ should be ordered to disgorge, for the benefit of the
27 Class, all or part of the ill-gotten gains it received from the sale of the Carrier IQ Software, and/or
28 to make full restitution to Plaintiffs and the Class.

1 54. Given: (i) the substantive complexity of this litigation; (ii) the size of individual
2 Class Members' claims; and (iii) the limited resources of the Class Members, few, if any, Class
3 Members could afford to seek legal redress individually for the wrongs Defendants have
4 committed against them.

5 55. Class treatment of common questions of law and fact would also be superior to
6 multiple individual actions or piecemeal litigation in that class treatment will foster an orderly and
7 expeditious administration of Class claims, economies of time, effort and expense, and uniformity
8 of decision.

9 56. This action presents no difficulty that would impede the Court's management of it
10 as a class action, and a class action is the best and/or the only available means by which members
11 of the Class can seek legal redress for the harm caused by Defendants.

12 57. Absent a class action, Class Members will continue to incur damages and
13 Defendants' misconduct will continue without remedy.

14 58. A class action is superior to other available methods for the fair and efficient
15 adjudication of the controversy.

16 59. The issues common to the claims of Plaintiffs and the Class Members, are
17 alternatively certifiable pursuant to Fed. R. Civ. P. 23(c)(4), as resolution of these issues would
18 materially advance the litigation, and class resolution of these issues is superior to repeated
19 litigation of these issues in separate trials.

20 **FIRST CAUSE OF ACTION**

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

22 60. This cause of action is brought on behalf of Plaintiffs and the Carrier IQ Subclass
23 against Defendant Carrier IQ; Plaintiff Daniel Pipkin and the Samsung Subclass against
24 Defendants Samsung and Carrier IQ; and Plaintiff Chad Ulrich and the HTC Subclass against
25 Defendants HTC and Carrier IQ.

26 61. Plaintiffs and Class Members incorporate by reference the allegations of the
27 preceding paragraphs of this Complaint as if set forth in full herein.

28 62. Defendants intentionally intercepted, or endeavored to intercept, electronic

1 communications of Plaintiffs and Class Members in violation of 18 U.S.C. §§ 2511, *et seq.* (the
2 “Federal Wiretap Act”). In addition, Defendants intentionally used, or endeavored to use, the
3 contents of electronic communications of Plaintiffs and Class Members, knowing that the
4 information was obtained through the interception of an electronic communication, in violation of
5 the Federal Wiretap Act.

6 63. The electronic communications Defendants intercepted and/or used were not made
7 through an electronic communication system that was readily accessible to the general public. To
8 the contrary, the very nature of the electronic communications Defendants intercepted and/or used
9 was private and confidential to Plaintiffs and Class Members.

10 64. As a direct result of Defendants’ conduct, pursuant to 18 U.S.C. § 2520, Plaintiffs
11 and Class Members are each entitled to: (1) statutory damages of whichever is the greater of \$100
12 a day for each day of violation or \$10,000 per Class Member; (2) punitive damages; (3) injunctive
13 or declaratory relief as deemed appropriate; and (4) reasonable attorneys’ fees and costs.

14 **SECOND CAUSE OF ACTION**

15 **VIOLATION OF COMPUTER FRAUD AND ABUSE ACT, (18 U.S.C. §§ 1030, *et seq.*)**

16 65. This cause of action is brought on behalf of Plaintiffs and the Carrier IQ Subclass
17 against Defendant Carrier IQ; Plaintiff Daniel Pipkin and the Samsung Subclass against
18 Defendants Samsung and Carrier IQ; and Plaintiff Chad Ulrich and the HTC Subclass against
19 Defendants HTC and Carrier IQ.

20 66. Plaintiffs and Class Members incorporate by reference the allegations of the
21 preceding paragraphs of this Complaint as if set forth in full herein..

22 67. All mobile devices equipped with the Carrier IQ Software operated by Plaintiffs
23 and Class Members are “computers” within the meaning of 18 U.S.C. § 1030(e)(1) because they
24 are high speed data processing devices that perform logical, arithmetic, or storage functions.

25 68. Plaintiffs’ and Class Members’ mobile devices are “protected computers” within
26 the meaning of 18 U.S.C. § 1030(e)(2)(B) because they are used in interstate commerce or
27 communication.

28 69. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030,

1 *et seq.*, by, *inter alia*: (1) intentionally accessing Plaintiffs' and Class Members' mobile devices
2 without authorization or exceeding authorized access, thereby obtaining information from their
3 mobile devices; (2) intentionally accessing Plaintiffs' and Class Members' mobile devices without
4 authorization, and as a result, recklessly causing damage; and/or (3) intentionally accessing
5 Plaintiffs' and Class Members' mobile devices without authorization, and as a result, causing
6 damage and loss.

7 70. Defendants intentionally accessed Plaintiffs' and Class Members' mobile devices
8 without authorization or exceeded their authorized access, and thereby obtained information from
9 their mobile devices. Defendants monitored, logged, and recorded the keystrokes Plaintiffs and
10 Class Members made in their mobile devices, obtaining information regarding Plaintiffs' and
11 Class Members' telephone calls, text messages, web browsing, and other activities.

12 71. Defendants intentionally accessed Plaintiffs' and Class Members' mobile devices
13 without authorization and recklessly caused damage by impairing the integrity of data or
14 information on their mobile devices. Specifically, Defendants' conduct jeopardized the private
15 and confidential nature of Plaintiffs' and Class Members' activities on their mobile devices.

16 72. Defendants intentionally accessed Plaintiffs' and Class Members' mobile devices
17 without authorization and caused damage and loss by forcing Plaintiffs and Class Members to
18 incur costs in responding to Defendants' offense, conducting a damage assessment, and/or
19 attempting to turn off, stop, or otherwise disable Defendants' software.

20 73. As a direct result of Defendants' conduct, Defendants obtained information valued
21 over \$5,000, caused damage exceeding an aggregate of \$5,000 in value during a one-year period,
22 and damaged 10 or more "protected computers" during a one-year period.

23 **THIRD CAUSE OF ACTION**

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

25 74. This cause of action is brought on behalf of Plaintiffs and Members of the Carrier
26 IQ Subclass Residing in California against Defendant Carrier IQ; Plaintiff Daniel Pipkin and
27 Members of the Samsung Subclass Residing in California against Defendants Samsung and
28 Carrier IQ; and Plaintiff Chad Ulrich and Members of the HTC Subclass Residing in California

1 against Defendants HTC and Carrier IQ.

2 75. Plaintiffs and Class Members incorporate by reference the allegations of the
3 preceding paragraphs of this Complaint as if set forth in full herein.

4 76. California Penal Code § 631 prohibits the intentional tapping of any telephone
5 instrument, including an instrument of any internal telephonic communication system, and the
6 unauthorized reading or learning, or attempted reading or learning, of any telephonic message,
7 report, or communication within the State of California.

8 77. Defendants have violated California Penal Code § 631 by monitoring, logging, and
9 recording private information from mobile devices without authorization. Defendants' software
10 monitors, logs, and records the keystrokes Plaintiffs and Class Members make on their mobile
11 devices, including phone numbers, text messages, and web browser searches.

12 78. Defendants' software is a "rootkit," meaning it hides itself from the user while
13 enabling privileged access to the user's cellular data. The software cannot be turned off or
14 stopped in some mobile devices, including Plaintiffs', and in fact, continues to log users'
15 keystrokes even when they disconnect their cellular connection and use a wireless connection.

16 79. Defendants' conduct constitutes the intentional tapping of a telephone instrument in
17 violation of California Penal Code § 631. It also constitutes the unauthorized reading or learning,
18 or attempted reading or learning, of telephonic messages and communications in violation of
19 California Penal Code § 631. Plaintiffs and Class Members have been injured by Defendants'
20 conduct in that their actions and private information on their cellular phones have been monitored,
21 logged, and recorded, jeopardizing the confidential nature of that information.

22 80. California Penal Code § 637.2 permits a civil action for violation of California
23 Penal Code § 631, authorizing an award of \$5,000 for each violation as well as injunctive relief.
24 Plaintiffs and Class Members are entitled to these remedies, and to attorneys' fees, as this lawsuit
25 seeks the enforcement of an important right affecting the public interest and satisfies the statutory
26 requirements for an award of attorneys' fees thereunder.

27 81. As a direct result of Defendants' conduct, Plaintiffs and Class Members have
28 sustained and will continue to sustain injury and are entitled to statutory damages and injunctive

1 relief to be determined at trial.

2 **FOURTH CAUSE OF ACTION**

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

4 82. This cause of action is brought on behalf of Plaintiffs and Members of the Carrier
5 IQ Subclass Residing in California against Defendant Carrier IQ; Plaintiff Daniel Pipkin and
6 Members of the Samsung Subclass Residing in California against Defendants Samsung and
7 Carrier IQ; and Plaintiff Chad Ulrich and Members of the HTC Subclass Residing in California
8 against Defendants HTC and Carrier IQ.

9 83. Plaintiffs and Class Members incorporate by reference the allegations of the
10 preceding paragraphs of this Complaint as if set forth in full herein.

11 84. California Penal Code § 632.7 prohibits the intentional recording of any
12 communication between cellular phones without the consent of all parties to the communication.

13 85. Defendants have violated California Penal Code § 632.7 by intentionally, and
14 without the consent of all parties to the communications, logging and recording communications
15 by Plaintiffs and Class Members on their cellular phones. Defendants' software monitors, logs,
16 and records the keystroke Plaintiffs and Class Members make on their cellular phones, including
17 text messages. Text messages are communications between cellular phones.

18 86. Defendants' conduct constitutes the intentional and nonconsensual recording of a
19 communication between cellular phones. Plaintiffs and Class Members have been injured by
20 Defendants' conduct in that their communications have been monitored, logged, and recorded,
21 jeopardizing the private nature of those communications.

22 87. California Penal Code § 637.2 permits a civil action for violation of California
23 Penal Code § 632.7, authorizing an award of \$5,000 for each violation as well as injunctive relief.
24 Plaintiffs and Class Members are entitled to these remedies, and to attorneys' fees, as this lawsuit
25 seeks the enforcement of an important right affecting the public interest and satisfies the statutory
26 requirements for an award of attorneys' fees thereunder.

27 88. As a direct result of Defendants' conduct, Plaintiffs and Class Members have
28 sustained and will continue to sustain injury and are entitled to statutory damages and injunctive

1 relief to be determined at trial.

2 **PRAYER FOR RELIEF**

3 WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated,
4 request the Court enter judgment against Defendants, as follows:


- 5 1. For an order certifying the Class, and appointing Plaintiffs and their counsel to
- 6 represent the Class;
- 7 2. For damages suffered by Plaintiffs and Class Members;
- 8 3. For preliminary and injunctive relief requiring Defendants to discontinue their
- 9 unauthorized access and recording of Plaintiffs' and Class Members' activities on their mobile
- 10 devices;
- 11 4. For reasonable attorneys' fees as permitted under applicable statutes;
- 12 5. For Plaintiffs' costs incurred;
- 13 6. For prejudgment interest; and
- 14 7. For such other and further relief which the court deems just and proper.

15 **DEMAND FOR JURY TRIAL**

16 Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs, on behalf of themselves and
17 all others similarly situated, demand a trial by jury of any and all issues in this action so triable.

18 DATED: December 2, 2011

19 **PEARSON, SIMON, WARSHAW & PENNY, LLP**
 20 CLIFFORD H. PEARSON
 21 BRUCE L. SIMON
 DANIEL L. WARSHAW
 AARON M. SHEANIN
 BOBBY POUYA
 THOMAS K. BOARDMAN

22 By: 
 23 DANIEL L. WARSHAW
 24 Attorneys for Plaintiffs, Daniel Pipkin and Chad Ulrich,
 25 on Behalf of Themselves and All Others Similarly
 26 Situated
 27
 28

PEARSON, SIMON, WARSHAW & PENNY, LLP
 15165 VENTURA BOULEVARD, SUITE 400
 SHERMAN OAKS, CALIFORNIA 91403

EXHIBIT “A”

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 website¹ (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

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

DDO

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.

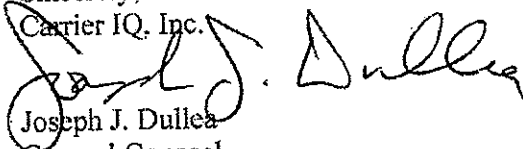
Before taking these steps, however, Carrier IQ, Inc. wishes to give you one opportunity to discontinue your illegal conduct by complying with this demand by 12.00pm EST on November 18th. Accordingly, please sign and return the attached *Agreement* by 12.00pm EST on November 18th to

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

EXHIBIT “B”



FOR IMMEDIATE RELEASE

Carrier IQ Press Statement

Mountain View, CA – November 23, 2011 – As of today, we are withdrawing our cease and desist letter to Mr. Trevor Eckhart. We have reached out to Mr. Eckhart and the Electronic Frontier Foundation (EFF) to apologize. Our action was misguided and we are deeply sorry for any concern or trouble that our letter may have caused Mr. Eckhart. We sincerely appreciate and respect EFF's work on his behalf, and share their commitment to protecting free speech in a rapidly changing technological world.

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

- Does not record your keystrokes.
- Does not provide tracking tools.
- Does not inspect or report on the content of your communications, such as the content of emails and SMSs.
- Does not provide real-time data reporting to any customer.
- Finally, we do not sell Carrier IQ data to third parties.

Our software is designed to help mobile network providers diagnose critical issues that lead to problems such as dropped calls and battery drain.

Here's what our software does:

- Our software makes your phone work better by identifying dropped calls and poor service.
- Our software identifies problems that impede a phone's battery life.
- Our software makes customer service quicker, more accurate, and more efficient.
- Our software helps quickly identify trending problems to help mobile networks prevent them from becoming more widespread.

We look forward to a healthy and robust discussion with EFF that we believe will be helpful to us, to our customers, and to consumers that use mobile devices. We welcome feedback on our products and understand that Mr. Eckhart and other developers like him play an important role by raising questions about the complicated and technical aspects of the mobile ecosystem.

EXHIBIT “C”

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