

ORIGINAL

1 Paul R. Kiesel, Esq. (SBN 119854)
 2 **KIESEL BOUCHER LARSON LLP**
 3 8648 Wilshire Boulevard
 4 Beverly Hills, CA 90211
 5 kiesel@kbla.com
 6 Telephone: (310) 854-4444
 7 Facsimile: (310) 854-0812

8 **HORWITZ, HORWITZ & PARADIS**
 9 **Attorneys at Law**
 10 570 Seventh Avenue, 20th Floor
 11 New York, NY 10018
 12 Telephone: (212) 986-4500
 13 Facsimile: (212) 986-4501
 14 (additional counsel listed on signature page)

15 **UNITED STATES DISTRICT COURT**
 16 **NORTHERN DISTRICT OF CALIFORNIA**

17 **EDWARD SHUMATE, individually**
 18 **and on behalf of all others similarly**
 19 **situated,**

20 **Plaintiff,**

21 **v.**

22 **CARRIER IQ, INC.**
 23 **A Delaware Corporation.**

24 **Defendant.**

E-Filing

ADR

FILED

DEC 13 2011

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

B
HH
See pl
Si

CASE NO. **V 11-06281**

HRL

CLASS ACTION COMPLAINT
FOR:

- (1) VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT;
- (2) VIOLATIONS OF THE CALIFORNIA PRIVACY ACT;
- (3) TRESPASS TO CHATTEL;
- (4) VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW; and
- (5) VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT

FAXED

1 Plaintiff Edward Shumate (“Plaintiff”) individually and on behalf of all others
2 similarly situated, by his undersigned counsel, alleges the following upon personal
3 knowledge as to his own acts and upon information and belief as to all other matters.
4 Plaintiff’s information and belief are based upon the investigation conducted by
5 counsel.

6 **NATURE OF THE ACTION**

7 1. Plaintiff brings this action individually and as a class action against Carrier
8 iQ, Inc. (“CiQ”) on behalf of himself and all others who either (i) own an electronic
9 device, including but not limited to, smartphones, traditional feature phones, tablet
10 computers, and electronic-readers (collectively the “Electronic Devices”) in which CiQ
11 Mobile Intelligence software (“CiQ’s software”) was installed, or (ii) own an Electronic
12 Device that sent an electronic communication to an electronic device in which CiQ’s
13 software was installed or received an electronic communication sent from an electronic
14 device in which CiQ’s software was installed.

15 2. Through its software, CiQ has been illegally intercepting, collecting, and
16 sharing the electronic communications that are sent and received by the Electronic
17 Devices in which CiQ is installed for several years.

18 3. Such electronic communications include every key that a user presses,
19 every text message and email sent and received by the user, and all Internet browser
20 usage and history while using the Electronic Devices.

21 4. This deeply intrusive surveillance campaign has occurred unbeknownst to
22 Plaintiff and Class members, who were not given an opportunity to provide informed
23 consent to such surveillance. The nature and extent of CiQ’s intrusive and
24 comprehensive surveillance was not disclosed to Plaintiff and the members of the Class.

25 5. As a result of the facts alleged herein, Defendant has violated federal and
26 state laws governing the protection of Plaintiff’s and Class members’ privacy.

27 \\\

28 \\\

1 **PARTIES**

2 6. Plaintiff Edward Shumate is a citizen of the State of Colorado. He
3 purchased three smartphones with cellular service provided by Sprint Nextel
4 Corporation (“Sprint”): an HTC Evo 4g, an HTC Evo 3D, and a Samsung Galaxy S2
5 Epic 4G Touch. Unbeknownst to Plaintiff, his devices all had CiQ’s electronic
6 communication interception software installed in them.

7 7. Defendant Carrier iQ Inc. maintains its principal executive offices at 1200
8 Villa Street, Suite 200, Mountain View, CA 94041. CiQ, established in 2005, develops
9 software that CiQ, cellular service providers (“carriers”), and original equipment
10 manufacturers (“OEMs”) use to collect and intercept data and communications sent or
11 received by a wide variety of Electronic Devices.

12 **JURISDICTION AND VENUE**

13 8. This Court has subject matter jurisdiction over the claims asserted in this
14 action pursuant to 28 U.S.C. § 1331 because Plaintiff’s claims arise under the laws of
15 the United States, including the Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*

16 9. This Court also has subject matter jurisdiction over the claims asserted in
17 this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332.
18 Plaintiff Edward Shumate, a citizen of Colorado, brings claims on behalf of a
19 nationwide class against Defendant, a citizen of California and the aggregate claims of
20 Plaintiff and members of the Class exceed the sum or value of \$5,000,000.

21 10. This Court has personal jurisdiction over Defendant because Defendant
22 maintains sufficient contacts in this jurisdiction.

23 11. Venue is proper in this District because Defendant maintains its principal
24 executive offices and headquarters in this District, and a substantial part of the events
25 giving rise to the claim occurred in this District.

26 \\\
27 \\\
28 \\\

1 **SUBSTANTIVE ALLEGATIONS**

2 **Background on the Smartphones and other Electronic Devices**

3 12. On its website, CiQ estimates that it has installed its CiQ software in more
4 than 140 million Electronic Devices.

5 13. A “smartphone” is a mobile phone that offers wireless internet connectivity
6 and more advanced computing ability than a traditional cellular phone. Because
7 smartphones have many of the features possessed by computers, smartphones require an
8 operating system (“OS”) to function. An operating system is software that consists of
9 programs and data that manages computer hardware resources and provides common
10 services for efficient execution of various application software.

11 14. A tablet is a class of small mobile computers, usually having a touchscreen
12 or pen-enabled interface. An e-reader is an electronic device for reading content, such
13 as books, newspapers and documents in digital format. Both e-readers and tablets have
14 wireless connectivity for downloading content and conducting other Web-based tasks.

15 15. The capabilities of the smartphones and the other Electronic Devices make
16 information accessible at the user’s fingertips. CiQ has capitalized on this technology
17 by using it to surveil Electronic Device users illegally 24 hours per day 7 days per
18 week, as admitted by CiQ’s own Vice President of Marketing, Andrew Coward.

19 16. According to CiQ’s website, “Our software is embedded by device
20 manufacturers along with other diagnostic tools and software prior to shipment.”
21

22 **CiQ’s Illegal Surveillance and Communication Interception**

23 17. CiQ’s software enables CiQ to read, intercept, and record all
24 communications that are sent and received by an electronic device in which CiQ’s
25 software is installed. Rather euphemistically, CiQ refers to its software and data
26 interception services as “Mobile Intelligence.”

27 18. Andrew Coward described the surveillance, data interception, and data
28 collection provided through CiQ’s software in detail when he stated in relevant part:

1
2 The answers lie within the handset itself because the handset holds untapped
3 information about what actually happens. Getting out and exploiting this
4 information is what we call 'mobile intelligence.' To extract it, we work
5 with handset manufacturers to embed an agent inside the phone—an agent
6 that works pretty much like a rewind button and records when things go
7 wrong and brings together the data to make them right again. So far this
8 agent has shipped on 150 million devices. And not just on handsets, but on
9 tablets, readers, and data sticks to provide detailed 'mobile intelligence' on
10 how well and where networks, devices, and applications are really
11 performing. . . .

12
13 19. CiQ's website states in relevant part:

14 Carrier IQ delivers Mobile Intelligence on the performance of mobile
15 devices and networks to assist operators and device manufacturers We
16 do this by counting and measuring operational information in mobile devices
17 – feature phones, smartphones and tablets. . . .

18
19 20. A CiQ press release described the illegal interception in great detail:

20 IQ Insight Experience Manager gives wireless carriers and mobile device
21 manufacturers an unprecedented, objective view into what is actually
22 happening on mobile subscribers' devices – including quality of service,
23 application usage and the related experience – as it occurs, at the point of
24 delivery and use.

25 * * *

26 Experience Manager takes customer experience profiling to an advanced
27 level with multiple levels of granularity, from the entire population, to
28 comparative groups, down to individual users

* * *

29 **IQ Insight Experience Manager uses data directly from the mobile**
30 **device to give a precise view of how the services and the applications are**
31 **being used, even if the phone is not communicating with the network.**

* * *

32 **The solution can be applied by Carrier IQ's existing customers to their**
33 **own deployed base of handsets which already have the company's core**
34 **technology embedded in the device, and it can also be applied to new**

1 devices as they are introduced. In total, Carrier IQ's core technology is
2 already embedded on more than 35 million handsets globally. (Emphasis
3 added).

4 **CiQ's Illegal Interception Scheme is Publicly Exposed**

5 21. In reality, CiQ's "Mobile Intelligence" amounts to illegal surveillance and
6 interception conducted without the consent of the Class members.

7 22. Electronic Device users were unaware that CiQ was illegally intercepting
8 their communications until a systems administrator, Trevor Eckhart, publicly revealed
9 the truth.

10 23. Trevor Eckhart explained that CiQ's software is a rootkit. A rootkit is
11 software that enables continued privileged access to a computer while actively hiding
12 its presence from administrators by subverting standard operating system functionality
13 or other applications.

14 24. He discovered that CiQ's software enables CiQ continued, privileged
15 access to the smartphones. CiQ's software is hidden in nearly every part of the
16 smartphones, including the kernel. The kernel is the main component of most computer
17 operating systems; it is a bridge between applications and the actual data processing
18 done at the hardware level. CiQ's software also subverts standard operating system
19 functionality.

20 25. Specifically, Trevor Eckhart discovered that CiQ's software was running in
21 his HTC Evo 3D smartphone. However, his smartphone would not allow him to disable
22 or remove CiQ's software.

23 26. Trevor Eckhart connected his smartphone to a device that allowed him to
24 observe the activity of the CiQ software, a process called USB debugging to read log
25 catalogue files created by the CiQ's software. The debugging log files were not only
26 stored in the operating system of the phone, but they were also transmitted to CiQ.

27 ///

28 ///

1 **A. CiQ Records Every Keystroke and Action**

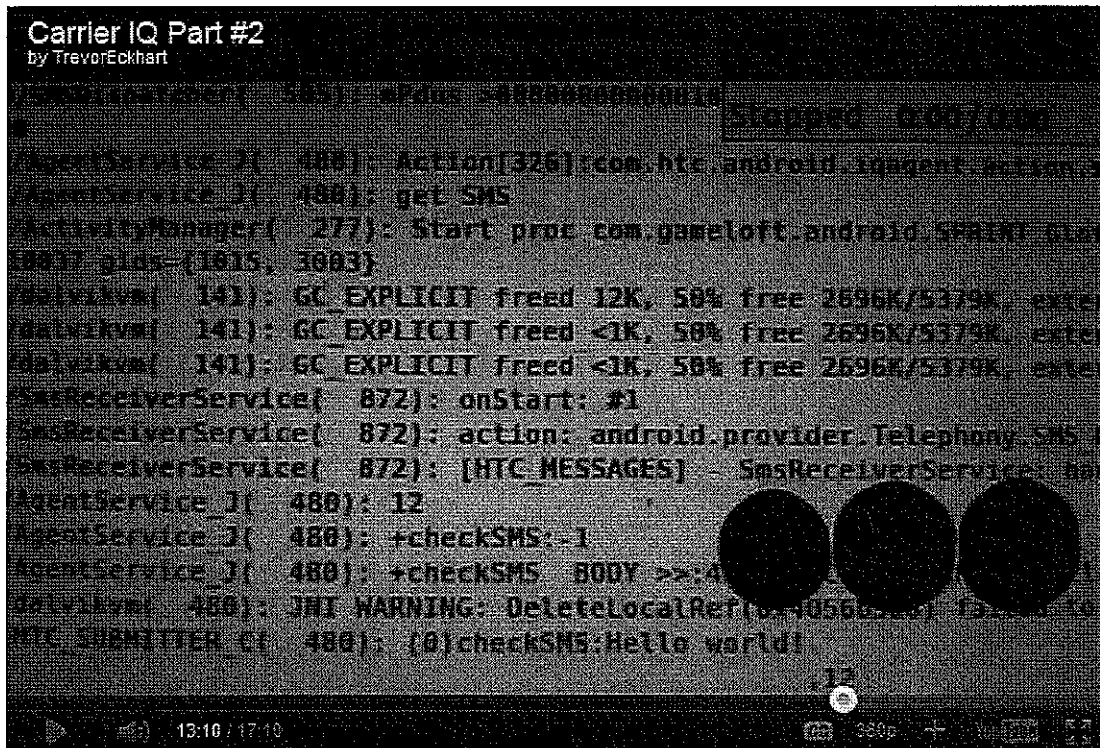
2 27. By depressing every button on his smartphone, Mr. Eckhart demonstrated
3 that a specific code called a “wkeycode” for each button was recorded and was sent to
4 CiQ. This enabled CiQ to recognize, read, and record every letter and word he typed
5 into his smartphone.

6 28. In addition, every action he took with his phone, such as turning it on or
7 off, had an action identifier. The action identifiers were also sent to CiQ
8 contemporaneously with their occurrence.

9 **B. CiQ Intercepts Every Text Message Sent and Received**

10 29. Using the USB debugger, Trevor Eckhart was able also to observe that
11 every time he sent or received a text message, CiQ was able to recognize that a text
12 message was sent or received and illegally intercept the text message. CiQ’s software
13 would then read and display the actual text of the text message to CiQ, as depicted in
14 **Figure 1** below at the bottom of the picture. In Trevor’s testing, that message was
15 “Hello World!”

16 **Figure 1**



1 30. CiQ's interception software is so sophisticated that it actually reads all text
2 messages sent from, or received by, an Electronic Device before the users of those
3 Electronic Devices are able to read them.

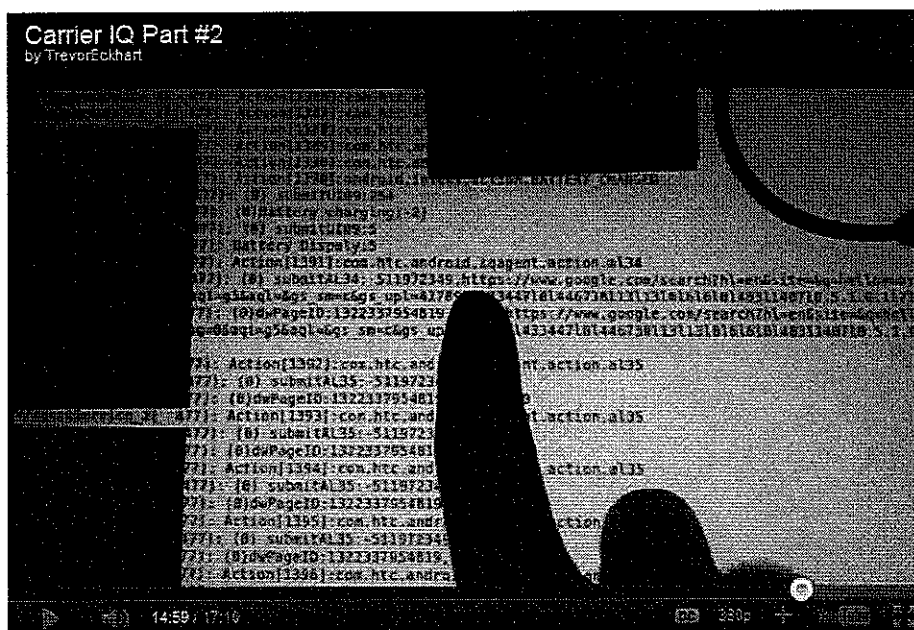
4 31. All of this information is then transmitted to not only CiQ, but also all of
5 CiQ's customers, which include OEMs and carriers.

6 32. CiQ's interception software is not unique to HTC smartphones. Rather,
7 CiQ software performs equivalent interception in any Electronic Device in which it is
8 installed. CiQ, by its own admission, is a data collector and data aggregator for its
9 customers.

10 11 C. CiQ Illegally Intercepts Internet 12 Communications on Private Wi-Fi Networks

13 33. Trevor Eckhart also discovered that CiQ illegally intercepted all Internet
14 browsing history while he was using his own wireless network, not his carrier's
15 network.

16 34. When Mr. Eckhart entered search terms into Google.com and performed an
17 Internet search, CiQ's software once again illegally intercepted these electronic
18 communications and actually read and displayed the search as depicted by **Figure 2**.



19 **Figure 2**

1 35. When a user enters search terms into a search engine or enters a URL into
2 the navigation toolbar, CiQ's software reads, records and transmits this information to
3 CiQ. CiQ, by its own admission, collects this data for its customers as well.

4
5 **D. CiQ's Software Could Not be Removed**

6 36. Eckhart discovered that, despite his efforts to disable CiQ software, it was
7 incapable of being disabled. Eckard had to design a new application specifically to
8 remove the CiQ's software because no other application with such power existed.

9 37. CiQ's software is programmed into the read only memory ("ROM") of the
10 smartphones' operating systems. Removing CiQ from the ROM requires gaining "root"
11 access to the ROM, which amounts to "unlocking" the ROM and is a risky procedure
12 that can damage the device.

13 38. As reported in the Wall Street Journal on December 5, 2011, by Tom
14 Loftus,

15 Because Carrier IQ software is deeply integrated with handset firmware,
16 users would be required to attain special device privileges in order to remove
17 it. Side effects of this process have the potential to put users at further risk of
18 malware infection while making devices ineligible to receive firmware
19 updates in the future.

20 39. The only other option to remove CiQ's software from the smartphone is to
21 remove and replace the ROM that is installed in the device by the manufacturer. The
22 user would have to obtain a newly designed ROM from another source.

23 40. CiQ's software also creates log catalogue files that that are stored within
24 the allocation of the operating system. These log catalogue entries consume space that
25 could be used for other applications and noticeably reduces the speed at which the
26 smartphone operates. After the log catalogue files are removed from the device, an
27 improvement in the rate of operation speed of the device is easily apparent.

28 \\

 \\

1 **E. CiQ's Half-Hearted Effort to Suppress**
2 **Trevor Eckhart's Discoveries**

3 41. When CiQ became aware that Mr. Eckhart was about to alert the public
4 about CiQ's illegal scheme, CiQ attempted to squelch Mr. Eckhart's activities by
5 serving him with a Cease-and-Desist letter, giving him two days to respond, and
6 threatening to seek damages from him if he did not cease his activities.

7 42. Undeterred by CiQ's threats, however, Eckhart hired the Electronic
8 Frontier Foundation, an organization committed to protecting privacy, to defend him.
9 Soon thereafter, CiQ withdrew its Cease-and-Desist letter and apologized to him,
10 stating that CiQ was "deeply sorry for any concern or trouble" that CiQ's Cease-and-
11 desist letter may have caused Eckhart.

12 43. Desiring to inform the public, Trevor posted his testing on YouTube.com.
13 His YouTube.com video of the software in action stunned many as it showed CiQ's
14 software logging information, including text messages, as the information is tapped
15 onto the phone keyboard.

16 44. After the shocking revelation, three major carriers admitted that CiQ's
17 software is embedded in their smartphones. AT&T publically acknowledged use of
18 CiQ's software. T-Mobile has also confirmed that CiQ's software is embedded in its
19 devices. T-Mobile, contacted by msnbc.com, said late Thursday, December 2, 2011, it
20 uses Carrier IQ. And Sprint Spokeswoman, Stephanie Vinge, admitted on behalf of
21 Sprint that CiQ's software is embedded in its smartphones and that CiQ supplies data to
22 Sprint.

23 45. The controversy caused by Trevar Eckhart's revelations also prompted
24 U.S. Senator Al Franken to send a letter to AT&T, HTC, Samsung, and Sprint Nextel,
25 after they acknowledged their use of CiQ's software, asking them to explain what they
26 do with the information that CiQ intercepts.

27 ///

28 ///

 ///

1 **Any Purported “Opt Out” or “Consent” is Deceptive and Invalid**

2 46. Carriers themselves do not disclose in their contracts the kind of
3 surveillance that Trevor Eckhart has shown CiQ to be performing.

4 47. Furthermore, CiQ has never entered into any agreement with Electronic
5 Device users, let alone obtained their consent to intercept their electronic
6 communications.

7 48. Moreover, no provision in any contract or service agreement for the
8 purchase of any electronic device in which CiQ’s software is installed disclosed to the
9 user that CiQ engages in the following: (i) CiQ will read and intercept all text typed into
10 the electronic device; (ii) CiQ will read and intercept all of the content of the user’s text
11 messages and emails, sent or received; and (iii) CiQ will read and intercept all internet
12 browsing history.

13 49. Without any disclosure of the intrusive and comprehensive nature of CiQ’s
14 communication interception, data collection, and surveillance, Plaintiff and Class
15 members were not capable of providing informed consent to CiQ.

16
17 **Plaintiff Shumate Detected**
18 **CiQ’s Software in His Electronic Devices**

19 50. Plaintiff never would have purchased the three Electronic Devices that he
20 purchased had he known of the existence and capability of CiQ’s software in his
21 smartphones.

22 51. It was not until software developers developed CiQ software detection
23 applications, after Eckhart exposed CiQ, that Plaintiff could discover the existence of
24 CiQ’s software embedded in his Electronic Device.

25 52. Plaintiff installed four different CiQ detection applications in all three of
26 his Electronic Devices. All four applications confirmed that his Electric Devices tested
27 positive for CiQ’s software. **Figure 3** is a screen capture of Plaintiff’s Samsung
28 smartphone depicting the test results of the CiQ detection software.

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

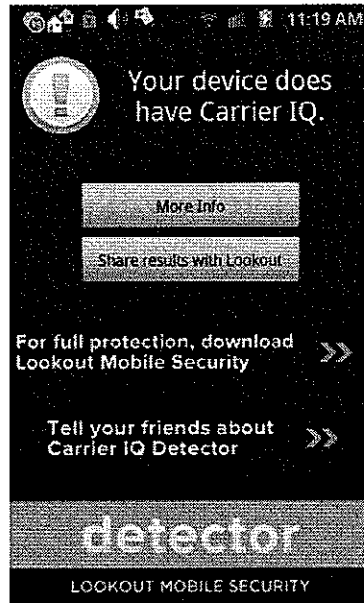


Figure 3

53. The CiQ detection applications did not have the power to remove CiQ’s software from the devices; they could only detect the presence of CiQ. One of such applications allowed Plaintiff to delete log catalogue files created by CiQ’s software that were entered into the ROM of Plaintiff’s smartphone.

54. After deletion of such files, Plaintiff noticed significant improvement in the speed at which his Electronic Device operated.

55. CiQ’s log catalogue files serve no purpose other than to transmit the contents of electronic communications to CiQ.

56. Even though Plaintiff could delete the log catalogue files after CiQ’s software created them, this deletion occurs only after the files have been transmitted to CiQ. Furthermore, no application has the power to prevent new log catalogue files from being created. After Plaintiff deleted the existing log catalogue files from his smartphone, CiQ immediately created new files.

User Outrage Over the Illegal Interception of Their Communications

57. Plaintiff and Class members reasonably expected that text messages, emails, and Internet browsing habits were private and confidential. They did not expect

1 or have knowledge that CiQ would illegally intercept and read their private
2 communications, much less share them with CiQ's customers.

3 58. As one incensed smartphone user exclaimed, "Stay out of my phone! And
4 reading my messages, everything I type even my id/passwords helps you support me
5 how? You say my information is secured, how and why would I trust you? You don't
6 give any option to opt-out or remove your spyware, and don't inform anyone what you
7 doing upfront, [expletive deleted]. I hope you get sued you [expletive deleted]."

8 59. Another smartphone user complained "A video by the aptly named
9 Andrew COWARD, pushing this program that has been lurking in my phone recording
10 every keystroke, website and message I get. Just how does this benefit me? I don't
11 remember signing up for this, and I certainly never gave you any sort of permission to
12 receive MY personal information that I pay a hefty amount per month to be able to send
13 and receive on MY phone. How you skirt legalities I haven't a clue, but I hope a lawsuit
14 is put together soon to put you out of business."

15 60. Yet another user echoed these sentiments, "OUT...OUT...STAY OUT OF
16 MY PHONE,LIERS...LIERS...LIERS [sic]...-DONT YOU DARE TO SAY WE DONT
17 UNDERSTAND [*]>>OFF...OUT THIEVES."

18 61. The following particular complaint reflects the concerns shared by other
19 Class members: "The reasons everyone are so up in arms about this: 1) The data you
20 collect goes well beyond data you need to help carriers support hardware/software. Why
21 do they need my text messages, google searches, and unencrypted login/password
22 details for my banking???? 2) You went to great lengths to hide this software on phones
23 and prevent users from turning it off. 3) Now that it has been exposed, you are
24 backpedaling and doing damage control after threatening to sue a user for simply
25 exposing you."¹

26
27
28

¹ User complaints are unedited to retain their authenticity.

1 66. The claims of Plaintiff are typical of the claims of the members of the
2 Class. Plaintiff has no interests antagonistic to those of the Class, and CiQ has no
3 defenses unique to the Plaintiff.

4 67. Plaintiff will protect the interests of the Class fairly and adequately, and
5 Plaintiff has retained attorneys experienced in complex class action litigation.

6 68. A class action is superior to all other available methods for this
7 controversy because:

- 8 a. the prosecution of separate actions by the members of the Class would
9 create a risk of adjudications with respect to individual members of the
10 Class that would, as a practical matter, be dispositive of the interests of the
11 other members not parties to the adjudications, or substantially impair or
12 impede their ability to protect their interests;
- 13 b. the prosecution of separate actions by the members of the Class would
14 create a risk of inconsistent or varying adjudications with respect to the
15 individual members of the Class, which would establish incompatible
16 standards of conduct for Defendant;
- 17 c. Defendant acted or refused to act on grounds generally applicable to the
18 Class; and
- 19 d. questions of law and fact common to members of the Class predominate
20 over any questions affecting only individual members, and a class action is
21 superior to other available methods for the fair and efficient adjudication of
22 the controversy.

23 69. Plaintiff does not anticipate any difficulty in the management of this
24 litigation.

25 ///

26 ///

27 ///

28 ///

1 **COUNT I**

2 **Violation of the Electronic Communications Privacy Act**
3 **Title 18 United States Code, Section 2510, *et seq.* (Wiretap Act)**

4 70. Plaintiff incorporates the above allegations by reference as if fully set forth
5 herein.

6 71. Defendant intercepted, tracked and recorded Plaintiff and Class Members'
7 electronic communications on Plaintiff and Class Members' Electronic Devices by and
8 through the use of Defendant's Carrier IQ software application. Defendant used this
9 software application to acquire the contents of Plaintiff and Class Members'
10 communications, thereby diverting and transferring information containing and
11 constituting the substance, purport, and meaning of Plaintiff and Class Members'
12 communications.

13 72. Defendant's conduct was in violation of Title 18, United States Code,
14 Section 2511(1)(a) because Defendant intentionally intercepted and endeavored to
15 intercept Plaintiff and Class Members' electronic communications.

16 73. Defendant's conduct was in violation of Title 18, United States Code,
17 Section 2511(1)(d) in that Defendant used and endeavored to use the contents of
18 Plaintiff and Class Members' electronic communications, knowing and having reason to
19 know that the information was obtained through interception in violation of Title 18,
20 United States Code Section 2511(1).

21 74. Defendant's conduct was knowing and intentional in that Defendant
22 designed and operated its Carrier IQ software application described herein and executed
23 this software application specifically for the purpose of engaging in the interceptions
24 that Defendant did, in fact, carry out.

25 75. Defendant was not a party to the respective communications between
26 Plaintiff and Class Members and websites, which Defendant monitored in-process.

27 76. Defendant's interception processes were invisible and unknown to Plaintiff
28 and Class Members.

1 77. Defendant failed to disclose its interception processes to Plaintiff and Class
2 Members.

3 78. Because Defendant's interception processes were invisible and
4 undisclosed, any consent Defendant received to participate in Plaintiff and Class
5 Members' communications did not constitute consent to Defendant's interception.

6 79. Only Plaintiff and Class Members possessed the authority to consent to
7 another party's interception of their electronic communications.

8 80. Defendant's interception was therefore undertaken without the consent of
9 any party to the communications that Defendant intercepted.

10 81. Defendant's tracking and interception of Plaintiff and Class Members'
11 electronic communications were not necessarily incident to Defendant's rendition of
12 services or protection of rights or property.

13 82. As a direct and proximate result of Defendant's conduct, Plaintiff and
14 Class Members' electronic communications were intercepted and intentionally used in
15 violation of Title 18, United States Code, Chapter 119.

16 83. Accordingly, Plaintiff and Class Members are entitled to such preliminary
17 and other equitable or declaratory relief as may be just and proper.

18 84. Plaintiff and Class Members are also entitled to damages computed as the
19 greater of: (i) the sum of actual damages suffered by Plaintiff and Class Members plus
20 Defendant's profits made through the violative conduct herein; (ii) statutory damages
21 for each Class Member of \$100 a day for each day of violation; or (iii) statutory
22 damages of \$10,000 per individual.

23 85. Plaintiff and Class Members are also entitled to and request Defendant's
24 payment of punitive damages.

25 86. Plaintiff and Class Members are also entitled to and hereby request
26 Defendant's payment of reasonable attorneys' fees and other litigation costs reasonably
27 incurred.

28 ///

1 **COUNT II**

2 **Violation of the Privacy Act**
3 **California General Laws, Chapter 214, Section 1B**

4 87. Plaintiff incorporates the above allegations by reference as if fully set forth
5 herein.

6 88. Defendant illegally intercepted, tracked and recorded Plaintiff and Class
7 Members' electronic communications as described herein.

8 89. Through the use of Defendant's Carrier IQ software application described
9 herein, Defendant disclosed to third parties, and/or caused to be disclosed to the other
10 third parties, Plaintiff and Class Members' Web-browsing, texting and calling
11 information, which included facts of a highly private, sensitive, personal or intimate
12 nature.

13 90. Defendant did so repeatedly throughout the Class Period.

14 91. Defendant did so knowing and intending to engage in conduct that Plaintiff
15 and Class Members did not reasonably expect.

16 92. Defendant did so knowing Plaintiff and Class Members reasonably
17 believed their privacy was protected. Defendant did so intending to circumvent the
18 measures Plaintiff and Class Members' had taken to protect their privacy.

19 93. Defendant did so knowing its actions would seriously diminish, intrude
20 upon, and invade Plaintiff and Class Members' privacy.

21 94. Defendant did so intending to seriously diminish, intrude upon, and invade
22 Plaintiff and Class Members' privacy.

23 95. Defendant did so in a manner designed to evade detection by Plaintiff and
24 Class Members.

25 96. Defendant had no legitimate, countervailing business interest in engaging
26 in such conduct.

27 97. Defendant' actions did unreasonably, substantially, and seriously interfere
28 with Plaintiff and Class Members' privacy.

1 106. By engaging in the acts alleged in this complaint without the authorization
2 or consent of Plaintiff and Class Members, Defendant dispossessed Plaintiff and Class
3 Members from use and/or access to their personal confidential information. Further,
4 these acts impaired the use, value, and quality of Plaintiff and Class Members' personal
5 confidential information. Defendant's acts constituted an intentional interference with
6 the use and enjoyment of Plaintiff and Class Members' personal confidential
7 information. By the acts described above, Defendant repeatedly and persistently
8 engaged in trespass to personal property in violation of the common law.

9 107. Without Plaintiff and Class Members' authorization or consent, or in
10 excess of any authorization or consent given, Defendant knowingly and intentionally
11 accessed Plaintiff and Class Members' property, thereby intermeddling with Plaintiff
12 and Class Members' right to exclusive possession of the property and causing injury to
13 Plaintiff and the members of the Class.

14 108. Defendant engaged in deception and concealment to gain access to
15 Plaintiff and Class Members' computers.

16 109. Defendant engaged in the following conduct with respect to Plaintiff and
17 Class Members' Electronic Devices: Defendant accessed and obtained control over
18 Plaintiff and Class Members' personal confidential information; Defendant caused the
19 installation of Defendant's Carrier IQ software application on Plaintiff and Class
20 Members' Electronic Devices; Defendant deliberately programmed the operation of its
21 software application code to bypass and circumvent the Electronic Device owners'
22 privacy and security controls, to remain beyond their control, and to continue to
23 function and operate without notice to them or consent from them. All these acts
24 described above were acts in excess of any authority Plaintiff and Class Members
25 granted when visiting websites and none of these acts was in furtherance of Plaintiff
26 and Class Members' viewing the content or utilizing services on websites. By engaging
27 in deception and misrepresentation, whatever authority or permission Plaintiff and Class
28 Members may have granted to the Defendant did not apply to Defendant's conduct.

1 110. Defendant's installation and operation of its program used, interfered,
2 and/or intermeddled with Plaintiff and Class Members' Electronic Devices. Such use,
3 interference and/or intermeddling was without Plaintiff and Class Members' consent or,
4 in the alternative, in excess of Plaintiff and Class Members' consent.

5 111. Defendant's installation and operation of its program constitutes trespass,
6 nuisance, and an interference with Plaintiff and Class Members' chattels, to wit, their
7 Electronic Devices and personal confidential information.

8 112. Defendant's installation and operation of its Carrier IQ software
9 application impaired the condition and value of Plaintiff and Class Member's Electronic
10 Devices and personal confidential information.

11 113. Defendant's trespass to chattels, nuisance, and interference caused real and
12 substantial damage to Plaintiff and Class Members.

13 114. As a direct and proximate result of Defendant's trespass to chattels,
14 nuisance, interference, unauthorized access of and intermeddling with Plaintiff and
15 Class Members' property, Defendant has injured and impaired in the condition and
16 value of Class Members' Electronic Devices and personal confidential information, as
17 follows:

- 18 a. by consuming the resources of and/or degrading the performance of
19 Plaintiff and Class Members' Electronic Devices (including hard drive
20 space, memory, processing cycles, and Internet connectivity);
- 21 b. by diminishing the use of, value, speed, capacity, and/or capabilities of
22 Plaintiff and Class Members' Electronic Devices;
- 23 c. by devaluing, interfering with, and/or diminishing Plaintiff and Class
24 Members' possessory interest in their Electronic Devices and personal
25 confidential information;
- 26 d. by altering and controlling the functioning of Plaintiff and Class Members'
27 Electronic Devices and personal confidential information;

- 1 e. by infringing on Plaintiff and Class Members' right to exclude others from
2 their Electronic Devices and personal confidential information;
- 3 f. by infringing on Plaintiff and Class Members' right to determine, as
4 owners of their Electronic Devices, which programs should be installed
5 and operating on their Electronic Devices;
- 6 g. by compromising the integrity, security, and ownership of Class Members'
7 Electronic Devices and personal confidential information; and
- 8 h. by forcing Plaintiff and Class Members to expend money, time, and
9 resources in order to remove the program installed on their Electronic
10 Devices without notice or consent.

11 115. Defendant's conduct constituted an ongoing and effectively permanent
12 impairment of Plaintiff and Class Members' Electronic Devices and personal
13 confidential information.

14 116. Plaintiff and Class Members each had and have legally protected, privacy
15 and economic interests in their Electronic Devices and personal confidential
16 information.

17 117. Plaintiff and Class Members sustained harm as a result of Defendant's
18 actions, in that the expected operation and use of their Electronic Devices and personal
19 confidential information were altered and diminished on an ongoing basis.

20 118. As a direct and proximate result of Defendant's trespass to chattels,
21 interference, unauthorized access of and intermeddling with Plaintiff and Class
22 Members' Electronic Devices and personal confidential information, Plaintiff and Class
23 Members have been injured, as described above.

24 119. Plaintiff, individually and on behalf of the Class, seek injunctive relief
25 restraining Defendant from such further trespass to chattels and requiring Defendant to
26 account for its use of Plaintiff and Class Members' Electronic Devices and personal
27 confidential information, account for the personal information they have acquired,
28 purge such data, and pay damages in an amount to be determined.

1 **COUNT IV**

2 **Violation of the Unfair Competition Law (“UCL”)**
3 **California Business and Professions Code § 17200, et seq.**

4 120. Plaintiff incorporates the above allegations by reference as if fully set forth
5 herein.

6 121. By engaging in the above-described acts and practices, Defendant has
7 committed one or more acts of unfair competition within the meaning of the UCL and,
8 as a result, Plaintiff and the Class have suffered injury-in-fact and have lost money
9 and/or property—specifically, personal confidential information and the full value of
10 their Electronic Devices and personal confidential information.

11 122. Defendant’s actions described above are in violation of California Business
12 and Professions Code section 17500, et seq. and violations of the right of privacy
13 enshrined in Article I, Section 1 of the Constitution of the State of California.

14 123. In addition, Defendant’s business acts and practices are unlawful, because
15 they violate the Electronic Communications Privacy Act and California Invasion of
16 Privacy Act. Defendant is therefore in violation of the “unlawful” prong of the UCL.

17 124. Defendant’s business acts and practices are unfair because they cause harm
18 and injury-in-fact to Plaintiff and Class Members and for which Defendant has no
19 justification. Defendant’s conduct lacks reasonable and legitimate justification in that
20 Defendant has benefited from such conduct and practices while Plaintiff and the Class
21 Members have suffered material disadvantage regarding their interests in the privacy
22 and confidentiality of their personal information. Defendant’s conduct offends public
23 policy in California tethered to the right of privacy set forth in the Constitution of the
24 State of California, and California statutes recognizing the need for consumers to obtain
25 material information with which they can take steps to safeguard their privacy interests.

26 125. Defendant’s acts and practices were also fraudulent within the meaning of
27 the UCL because they are likely to mislead the members of the public to whom they
28 were directed.

1 intentional recordation of, a communication transmitted by and between the Electronic
2 Devices. (Cal. Pen. Code § 632.7(a).)

3 132. Penal Code Section 637.2 is a manifestation of the California Legislature's
4 determination that the privacy invasion arising from the non-consensual interception,
5 wiretapping, eavesdropping, or recording of a confidential communication constitutes
6 an affront to human dignity that warrants a minimum of \$5,000 in statutory damages
7 per violation, even in the absence of proof of actual damages, as well as injunctive relief
8 enjoining further violations. (Cal. Pen. Code § 637.2(a)-(c).) Defendant's unlawful
9 conduct caused injury to Plaintiff and the Class in the form of an affront to their human
10 dignity.

11 133. Based upon the foregoing, the Class members, including the Plaintiff, are
12 entitled to, and below do pray for, statutory damages for each of Defendant's violations
13 of Penal Code Sections 631, 632.7 and for injunctive relief, as provided under Penal
14 Code Section 637.2.

15
16 **PRAYER FOR RELIEF**

17 **WHEREFORE**, Plaintiff prays that this Court:

18 a. Certify this action as a class action under Rule 23 of the Federal Rules of
19 Civil Procedure, appoint the named Plaintiff as the Class representative, and appoint the
20 undersigned as class counsel;

21 b. Order Defendant to pay Plaintiff and other members of the Class an
22 amount of actual and statutory damages, restitution and punitive damages in an amount
23 to be determined at trial;

24 c. Issue a permanent injunction or other appropriate equitable relief requiring
25 Defendant refrain from its ongoing illegal interception and other activities;

26 d. Issue an order granting Plaintiff's reasonable costs and attorney's fees; and

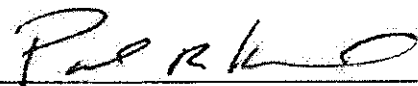
27 e. Grant such other relief as may be just and proper.

28 ///

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

Dated: December 13, 2011

KIESEL BOUCHER LARSON LLP

By: 

Paul R. Kiesel, Esq. (SBN 119854)
KIESEL BOUCHER LARSON LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

Paul O. Paradis, Esq.
Gina M. Tufaro, Esq.
Mark A. Butler, Esq.
pparadis@hhplawny.com
HORWITZ, HORWITZ & PARADIS,
Attorneys at Law
570 Seventh Avenue, 20th Floor
New York, NY 10018
Telephone: (212) 986-4500
Facsimile: (212) 986-4501

James v. Bashian, Esq.
Law Offices of James V. Bashian
500 Fifth Avenue – Suite 2700
New York, New York
(212) 921-4110

Counsel for Plaintiff

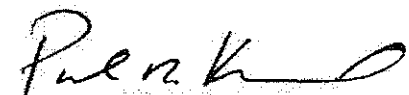
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

Dated: December 13, 2011

KIESEL BOUCHER LARSON LLP

By: 
Paul R. Kiesel, Esq. (SBN 119854)
KIESEL BOUCHER LARSON LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

Paul O. Paradis, Esq.
Gina M. Tufaro, Esq.
Mark A. Butler, Esq.
pparadis@hhplawny.com
HORWITZ, HORWITZ & PARADIS,
Attorneys at Law
570 Seventh Avenue, 20th Floor
New York, NY 10018
Telephone: (212) 986-4500
Facsimile: (212) 986-4501

James v. Bashian, Esq.
Law Offices of James V. Bashian
500 Fifth Avenue – Suite 2700
New York, New York
(212) 921-4110

Counsel for Plaintiff