Daniel Low (SBN 218387; dlow@kotchen.com)
KOTCHEN & LOW LLP
2300 M. Street NW, Suite 800
Washington, DC 20037
Telephone (202) 416-1848
Facsimile: (202) 280-1128

Attorney for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

PLAINTIFFS SAM STOLTENBURG and AMBER WESTENBERGER, on behalf of themselves and all others similarly situated,

Plaintiffs,
v.

CARRIER IQ, INC., LG ELECTRONICS U.S.A., INC., LG ELECTRONICS MOBILECOMM U.S.A., INC., and LG ELECTRONICS MOBILE RESEARCH U.S.A., LLC,

Defendants.

Civil Action No. CV 11-06160

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Introduction

1. This case involves Defendants' use of hidden software on Plaintiffs' smartphones to obtain, monitor and transmit data from the smartphones in violation of the Federal Wiretap Act as Amended by the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et. seq.

The Parties

2. Plaintiff Sam Stoltenburg is a Wisconsin citizen.

3. Plaintiff Amber Westenberger is a Wisconsin citizen.

4. Defendant Carrier IQ, Inc. ("CIQ") is a Delaware corporation with its principal place of business and headquarters in Mountain View, California, and also has offices in Chicago, IL, Boston, MA, London, UK, and Kuala Lumpur (Malaysia). CIQ creates and sells software that is installed on cell phones, smartphones, and other electronic devices throughout the United States, including software installed on smartphones purchased and used by Plaintiffs as referenced herein.

5. Defendant LG Electronics U.S.A., Inc. is a Delaware corporation with its principal place of business in Englewood Cliffs, NJ.

6. Defendant LG Electronics MobileComm U.S.A, Inc. is a California corporation with its principal place of business in San Diego, CA.

7. Defendant LG Electronics Mobile Research U.S.A., LLC is a California corporation with its principal place of business in San Diego, CA.

8. Defendants LG Electronics U.S.A., Inc., LG Electronics MobileComm U.S.A, Inc., and Electronics Mobile Research U.S.A., LLC (collectively "LG") are affiliated companies involved in the manufacture of cell phones and smartphones throughout the United States, and including smartphones purchased and used by Plaintiffs as referenced herein.

Jurisdiction, Venue and Interstate Commerce

9. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 (federal question). This Court also has jurisdiction pursuant to 28 U.S.C. § 1332 (diversity jurisdiction), because this action is brought as a class action, diversity of citizenship exists between the parties, and the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs.

10. Venue in this District is proper pursuant to 28 U.S.C. § 1391, in that Defendants (either currently or during the relevant time period of this Complaint) inhabit, transact business, reside, are found, or have an agent in this district; a significant portion of the affected interstate trade and commerce described below has been carried out in this District; and a substantial part of the events giving rise to Plaintiffs' claims occurred in this District.

11. Defendants' fraudulent activities were within the flow of and had a proximate, direct, substantial, and reasonably foreseeable effect on interstate commerce.

12. Relief is sought against Defendants as well as their employees, agents, assistants, and successors.

Factual Allegations

CIQ's Software, As Marketed to Its Customers, Including Device Manufacturers Like LG

13. Through its software, CIQ has been illegally, intercepting, collecting and sharing electronic communications of Plaintiffs and the Class. CIQ's intrusive surveillance has occurred unbeknownst to and without the consent of Plaintiffs and the Class.

14. CIQ's website describes CIQ's business of gathering and storing information of mobile phone users:

> Carrier IQ enables mobile operators, mobile device manufacturers, application vendors and other participants in the Mobile Ecosystem to deliver high quality products and services, based on what you want, where you want and to work and perform the way you expect.
>
> In providing our products and services, Carrier IQ enables our customers to gather information on Mobile User Experiences…
>
> …
>
> With deployment on over 130 million phones globally, we have considerable experience in protecting the privacy of the end user and doing so in a highly secure manner. Information transmitted from enabled mobile devices is stored in a secure data center facility that meets or exceeds industry best practice guidelines for security policies and procedures.
>
> http://carrieriq.com/company/privacy.htm

15. Another CIQ webpage states:

> Carrier IQ solutions address the needs of device OEMs [original equipment manufacturers], mobile network operators, mobile virtual network operators, enterprises and content providers to provide higher quality services and products to their end customers. …
>
> …
>
> Carrier IQ solutions deliver critical information to the device OEMs' and operators' decision makers across key business units and divisions. …

> . . .
> Carrier IQ solutions combine device-resident software and server-side business analytics applications to provide actionable intelligence on end-user customer experience, performance and service quality. The embedded device agents are currently shipped on more than 75 million devices across numerous device manufacturers and models. The solutions can be deployed across multiple wireless technologies such as CDMA2000, GSM, UMTS/WCDMA, WiFi, and device types such as feature phones, smart phones, PDAs, data cards.
>
> http://carrieriq.com/company/careers.htm

16. Another CIQ webpage similarly states:

> Carrier IQ's Mobile Service Intelligence solution eliminates guesswork by automatically providing accurate, real-time data direct from the source – your customers' handsets. Our powerful platform aggregates, analyzes and delivers that data via easy-to-use web applications that help wireless carriers make smart business decisions. The kind that can dramatically accelerate time to market, reduce operating costs and increase customer satisfaction across every division – marketing, sales, development, customer service, operations, and executive management – and every business unit – device, network and application.
>
> Carrier IQ is unique in the wireless industry because we are the only company embedding diagnostic software in millions of subscribers' phones. And, we are the only ones who add the "IQ" or smarts to the data. This is Actionable Intelligence – information and analysis you can use to identify problems and more importantly, solve them. And, we are a proven leader with millions of handsets deployed with Carrier IQ software inside.
>
> http://carrieriq.com/overview/index.htm

17. CIQ describes how it processes raw data (which CIQ calls "Metrics") collected from devices, and ways customers can use the data:

> Carrier IQ's Mobile Service Intelligence Platform (MSIP) is the smart database at the heart of our solution. It receives raw data (known as Metrics) from phones and converts them into reliable, repeatable Measures which feed into analytic applications. The MSIP delivers true enterprise grade performance, with its proven ability to process data submitted by millions of phones with outstanding integrity and security.

> …
> We know you don't just want data, you want to solve business problems and identify new business opportunities. The IQ Insight application suite uses data from the MSIP to deliver true Actionable Intelligence, tailored to specific business areas. From the performance information to support the launch of a new phone or service to historical information to understand in detail customer behavior and usage patterns, the IQ Insight suite cuts through the complexity to allow you to focus on critical business issues, create and track Key Performance Indicators (KPIs) and all in the knowledge that the data is measured at the point the customer experienced it – in the phone.
>
> What's more, the combination of the MSIP and IQ Insight lets you move seamlessly from broad trend data across many users, through comparative groups down to diagnostic data from individual devices. Now, not only can you identify trends, you have the power to drill down to specific instances, giving you the insight your specialists need to make a difference. That is the power of Mobile Service Intelligence.

http://carrieriq.com/overview/mobileservice/index.htm.

Individual-Identifiable Data at the Keystroke Level; Video Demonstrating the Same

18. As CIQ admits above, CIQ collects and provides data for its corporate customers (including manufacturers) that include "data from individual devices," i.e. data identifiable to individual cell phones and the specific mobile users (including Plaintiffs) who use them.

19. As CIQ admits above, CIQ collects and provides data for its corporate customers (including manufacturers) that include "historical information to understand in detail [device user/customer] behavior and usage patterns." Coupled with CIQ's software's ability to identify data from individual phones, this means "historical" and "behavioral" data of individual device users are obtained and maintained by CIQ for its corporate customers' use.

20. In fact, CIQ's software collects and analyzes highly-personalized and detailed information from a given individual user's phone device. For example, CIQ asserts "IQ Insight Device Analyzer gives you more than just data: it provides a visualization of activity at all layers within the device." http://carrieriq.com/overview/IQInsightDeviceAnalyzer/index.htm.

21. CIQ filed a patent application that included claims related to a methodology for collecting device-users' key strokes:

> 8. The method of claim 2, wherein the set of data relates to a service of the communications network that is provided to an end user through the device.
>
> 9. The method of claim 2, wherein the set of data relates to a usage history of the device.
>
> 10. The method of claim 2, wherein the set of data relates to an end user's interaction with the device.
>
> 11. The method of claim 10, wherein the interaction with the device comprises the end user's pressing of keys on the device.

http://www.faqs.org/patents/app/20110106942.

22. The CIQ software's collection of a device-user's key strokes was demonstrated in a video created by Trevor Eckhart, a software application worker who investigated CIQ. Mr. Eckhart publicly revealed the truth about CIQ's invasive technology, posting his video at the following website: http://www.youtube.com/watch?v=T17XQI_AYNo

23. As Mr. Eckhart discusses and demonstrates in the video:

a. His smartphone is a "stock" device and factory-reset before he begins his demonstration;

b. His device has an Android (Google) operating system;

c. His device is "non-rooted" which means he cannot change the files that make up the operating system;

d. His device was manufactured by HTC;

e. He indicates "we've seen stock clients on" other manufacturers' devices;

f. In the menu list of "All" Applications and their icons, CIQ's software is not visible amongst the applications (which include applications by manufacturer HTC and by other parties, e.g. Adobe Reader);

g. An example application included on the device, Adobe Reader, prompts a privacy policy notice shortly after its icon is clicked the first time;

h. Only when he examines a system performance measure, to see which applications are actually running on the phone, does he see the first reference (indirectly at that) to CIQ's software's existence on the phone;

i. The CIQ software is indirectly referenced in a running application with a nondescript icon titled "HTC IQAgent";

j. When that "HTC IQAgent" application is opened, it indicates "No permission [is] required" for the "HTC IQAgent" application;

k. When the "About" button is clicked, a screen opens which shows an HTC logo, even though the "HTC IQAgent" application is not (he says he was told by HTC) HTC software;

l. The CIQ software is indirectly referenced in another running application titled "IQRD", which has the same nondescript icon as the "HTC IQAgent" had as referenced above;

m. The "IQRD" application was not initially present in the list of running applications, and only appeared after he opened the "HTC IQAgent" icon;

n. The Permissions area states "This application can access the following on your phone" … "Your Personal Information," "Services that Cost You Money," "Your Messages," "Your Location," "Network Communication," "Storage," "Phone Calls," "Hardware Controls," and "System Tools;"

o. The "IQRD" application is set such that it is always running when the Android operating system is running;

p. The "Force Stop" button (which presumably should stop the application) does not work, and the "IQRD" application keeps running;

q. In the Legal Information area of the phone, there is reference to Sprint, HTC and Google, but no reference to Carrier IQ;

r. Going to a log screen, he types different keys on his phone and shows how the IQRD application logs individual key strokes he enters and submits each key stroke (with a U101 and unique key code identifying the key stroke) to the IQRD application;

s. Going to a log screen, he shows how a test SMS text message he receives (including its content, the test phrase "Hello world!") is dispatched to CIQ's IQRD application, as indicated by dispatch language on the log, e.g. "dispatchSmsToCIQ…"

t. The SMS text is sent to the CIQ application before it even appears for his (the user's) own view;

u. He shows how when he uses an internet browser and visits the website www.google.com, while on a WiFi network and off of any cell carrier network, his location is submitted to the CIQ application;

v. His location was submitted to the CIQ application even though he had declined permission for Google (whose website he was at) to send his location information elsewhere;

w. The url of the webpage (www.google.com) he was visiting was sent to the CIQ application as well;

x. While at the google.com website, he enters the phrase "hello world" as a Google search phrase, and finds CIQ's application querying the search string "hello world" (which is supposed to be encrypted per presence of https://) over a wireless/WiFi/non-cell network, and nonetheless logs and submits the search string information, unencrypted, to CIQ's application.

24. According to CIQ's website, CIQ's software (installed on over 75 million mobile devices) transmits device-users' data to CIQ's "data center facility." http://carrieriq.com/company/privacy.htm

25. CIQ asserts its data center facility that receives device users' data is "secure," and that "techniques" are used to protect privacy and implement security, "including anonymization of

certain user-identifiable data, aggregation of data and encryption of data, etc." http://carrieriq.com/company/privacy.htm

26. However, CIQ's website information reveals that these techniques (such as anonymization or encryption) are often optional, with their use or non-use placed in the control of CIQ's paying customers who are given access to device users' data. As a CIQ webpage states, CIQ's *customers*— i.e. manufacturers, operators, vendors and others—have customized control over how CIQ's collected device data is used. For example, CIQ's website lists the following highly-customizable "Features" that corporate customers can use with CIQ's IQ Insight Device Analyzer:

> - Measure quality, reliability, performance, and characteristics of devices and services.
>
> . . .
>
> - Define device profiles, which specify the event data to be submitted, as well as the circumstances that trigger capture.
>
> . . .
>
> - Run custom reports to address your needs.
> - Manage events and measures based on trial goals.

http://carrieriq.com/overview/IQInsightDeviceAnalyzer/DeviceAnalyzer.datasheet.pdf

27. Thus, while it's true that corporate customers can choose to limit some "custom" data gathering and reports to aggregated, anonymous or encrypted information, as is CIQ's preferred public point of emphasis, they can also choose to access highly individualized phone/user data as referenced above (e.g. individual cell user's keystrokes or unencrypted web-search-string words or webpages visited), and to access CIQ's custom analyses of the same data.

28. CIQ's webpage admits that CIQ collects individualized data:

> IQ Insight gives you more than just data – it provides the monitoring and drill-down capabilities to move seamlessly from analysis of a group of devices containing as many as several million active users, through to detailed inspection of data from specific devices and events of interest. The ability to switch effortlessly from the "telescope" view of a population of a large number of users right down to "microscope" analysis of individual devices and events is a unique capability of IQ Insight.
>
> http://carrieriq.com/overview/IQInsightDatacardAnalyzer/index.htm

Transmission of the Data to CIQ for Corporate Customers' Use

29. CIQ's transmission of mobile user's data is described by Mr. Eckhart as follows:

> Gathering information from the [CIQ] training videos, we see everything is broken down into two categories – Metrics and Triggers.
>
> Metrics appears to be what data to log/send when a trigger is encountered. From the functions we have found already on our devices we knew the list was big, but even the below list only begins to scratch the surface.
>
> Triggers appear to be when to collect metrics. For example when a user installs or opens an app any given metric can be called getting information. When a user browses a webpage HTTP header information can be grabbed along with detailed information on the page, or CarrierIQ can log keypresses made on what webpage. When location is changed the phone can report in. When a call is placed or data is started any metrics can be queried. There is alot more, these are just what was shown in public documents. These triggers seem to be menu items shown in the hidden Carrier IQ Test UI.
>
> ...
>
> As mentioned before, Carrier IQ is rootkit software. It listens on the phones for commands contained in "tasking profiles" sent a number of ways and returns whatever "metric" was asked for.

http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/

30. According to patent information from CIQ titled "Collection of data at target wireless devices using data collection profiles" at the website http://www.patents.com/us-7609650.html:

> After the target devices have been identified, the process 800 advances to stage 816 where the new or updated profile, as applicable, is transmitted to the identified target device(s). Profile transmission can occur in a variety of ways, including "pushing" the data collection profile to the target device, sending a message, such as an SMS, to the target device prompting it to retrieve the data collection profile, and preparing the data collection profile for download the next time the target device contacts SQP 201 such as when it uploads a metrics package. Such profile transmission to the SQC 402 residing on the target device(s) may be achieved using any of a variety of transport mechanisms and standards including Short

Message Service ("SMS"), Hypertext Transport Protocol ("HTTP"), Hypertext Transport Protocol Secure ("HTTPS"), Wireless Application Protocol ("WAP") Push, IP-based Over-the-Air (IOTA) protocol, OMA/DM, or other protocols that are known in the art or that may be developed in the future.

The process 800 then advances to stage 818 where the data collection profile is stored on the target devices. When received by a target device, the collection profile is processed by SQC 402. In some cases, the data collection profile may be stored as received, or integrated with or take the place of previously received data collection profile(s). Factors that affect the how the data collection profile is processed by SQC 402 include, but are not limited to, the suitability of the device to the data collection requirements defined in the data collection profile, the relative priority of the data collection profile and any previously received profiles, and any explicit processing rules stated in the data collection profile. If processing the new profile by SQC 402 results in the data collection activity differing in any way from that specified in the data collection profile (e.g. if the device self-selects out of the data collection activity), SQC 402 may communicate back to SQP 201 the specifics of how and why the data collection activity differed.

The data collection profile can be transmitted to the target devices over a wireless or wireline connection. Because the data collection profile is relatively small, the transmission of the data collection profile proceeds relatively quickly and imposes minimal processing overhead on the target devices. Further, the population of target devices can be quickly redefined and data collection profiles quickly and easily downloaded in order to achieve data collection goals. Such iterative data collection processes are particularly useful in understanding transient error conditions because of the speed with which the data collection activity can be refined. Other data collection activities may contribute to more long term trend analyses. For example, thresholds might be set with regard to performance degradation that, when reached, would cause generation and download of a data collection profile to a population of wireless devices. In this manner, additional data collection can take place that would enable further exploration of the problem. Consequently, embodiments of the data collection and management system are highly flexible and data collection efforts can be quickly refined, reconfigured, and redirected in response to rapidly emerging network conditions or transient network conditions. In any case, statistical analyses performed in connection with the collected data can rapidly converge on a solution or answer to the question posed in connection with the query.

> Unlike systems known in the art, the data collection and management system does not rely on the end users of the target devices to download the data collection profiles or to otherwise take action to enable the data collection process. Rather, as indicated above, the update of the target devices proceeds with minimal or no involvement on the part of the end user of the target device. Moreover, because each target device has been carefully qualified for participation in the data collection activity, the likelihood that any particular target device is not a valid candidate for a collection task is minimized. Thus, the collection of data as specified in connection with the data collection and management system 200 is performed quickly and easily by the target devices. Moreover, because the data collection profile is typically generated automatically in response to the occurrence of certain network conditions, the flexibility and speed with which the data collection management system 200 operates is further enhanced.

31. Mr. Eckhart describes the nature of the data collected by CIQ, and explains that the existence of the CIQ software is hidden from mobile users:

> IQ Insight Experience Manager uses data directly from the mobile device to give a precise view of how the services and the applications are being used, even if the phone is not communicating with the network. (From http://www.carrieriq.com/company/PR.Experience_Manager.CTIA-09.090325.pdf)
>
> . . .
>
> From training documents found we get an insight to the Carrier IQ Portal. Devices are displayed to the portal operator by individual phone Equipment ID and Subscriber IDs. The "portal administrator" can put devices into categories and see devices in California that have dropped calls at 5pm.
>
> . . .
>
> The down side to all of this is the "portal administrator" is also able to "task" a single phone with a profile containing any combinations of metric and trigger. From leaked training documents we can see that portal operators can view and task metrics by equipment ID, subscriber ID, and more. So instead of seeing dropped calls in California, they now know "Joe Anyone's" location at any given time, what he is running on his device, keys being pressed, applications being used.
>
> . . .
>
> Why do you keep calling CarrierIQ a rootkit?
>
> The definition of rootkit from wikipedia is exactly what CarrierIQ is.

> > A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool)
>
> CarrierIQ as seen in real world usage (HTC Devices especially) is nothing like the stock copies shown on the first page. All menus have been stripped, hiding it from users presence without advanced knowledge. The service also runs as user Root in ramdisk. It checks in to a server (or receives commands through other various access) with commands to allow someone undetected access.
>
> ...
>
> The only way to remove Carrier IQ is with advanced skills.

http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq

Plaintiffs' Purchase of LG Smartphones With Hidden CIQ Software Installed

32. In approximately early September 2011, Plaintiffs Stoltenburg and Westenberger each purchased cell service plans from cell carrier Sprint, along with cell phones of the model LS670 (hereafter "smartphones") manufactured by LG.

33. Unbeknownst to the Plaintiffs, their smartphones came embedded with software created by CIQ.

34. To Plaintiffs' knowledge and recollection, they were never informed of the CIQ software being on their phones, or given notice or a chance to grant permission for, the CIQ software to run any application(s) on their phones.

35. The (hidden) presence and operation of CIQ software on Plaintiffs' smartphones are similar in material respects to those of the CIQ software on Mr. Eckhart's phone as detailed above, with the material exception that LG is the manufacturer of Plaintiffs' phones, and plays an equivalent role as that of HTC referenced above.

36. Plaintiffs have repeatedly and consistently used their smartphones for many user functions as referenced above, including but not limited to SMS texting, phone calls, web browsing, and internet- and Google- searches. As a result of this, and as a result of the CIQ and LG Defendants' use and involvement with the CIQ software, Plaintiffs have had their wire, oral,

and/or electronic communications intentionally and unlawfully intercepted, used and disclosed by Defendants CIQ and LG who each knew or had reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of 18 U.S.C. § 2511. Also, Defendants' actions and CIQ's unwanted software have caused Plaintiffs to incur losses, such as (in the words of CIQ) the "incurring of processing overhead on the target devices," "performance degradation" on their devices, more rapid loss of battery power, and other performance problems.

Class Action Allegations

37. Plaintiffs bring this action, pursuant to Fed. R. Civ. P. 23, on behalf of the following class and subclass:

> **Carrier IQ Class**
> All persons in the United States who have owned smartphones, cell phones, tablets, or other devices from which CIQ collected electronic communications without their knowledge or consent.
>
> **LG Subclass**
> All persons in the United States who have owned smartphones, cell phones, tablets, or other devices manufactured by LG from which CIQ collected electronic communications without their knowledge or consent.

38. Excluded from the class are the Court and its officers, employees and relatives, Defendants and their parents, subsidiaries, affiliates, employees and co-conspirators, and government entities.

39. Members of the class are so numerous and geographically dispersed that joinder is impracticable. While the exact number of class members is unknown to Plaintiffs, based on Defendant CIQ's representations above, there are likely millions of class members. Members of the class are readily identifiable from information and records in possession of the Defendants.

40. Questions of law and fact common to members of the class predominate over questions, if any, that may affect only individual class members because Defendants have acted on grounds generally applicable to the class. Such generally applicable conduct is

inherent in Defendants' wrongful conduct. Common questions of law or fact include, but are not limited to:

a. Whether CIQ software installed on Class members' smartphones and other electronic devices has logged, intercepted, used, disclosed and transmitted information from those devices without the users' permission;

b. Whether Defendants' conduct violates the Federal Wiretap Act as Amended by the Electronic Communications Privacy Act, 18 U.S.C. 2510 et. seq.;

c. Whether Plaintiffs and other class members have sustained or continue to sustain damages as a result of Defendants' wrongful conduct, and, if so, the proper measure and appropriate formula to be applied in determining such damages;

d. Whether Plaintiffs and the other class members are entitled to an award of statutory damages, and, if so, in what amount; and

e. Whether Plaintiffs and the other class members are entitled to injunctive or other equitable relief.

41. Plaintiffs' claims are typical of the claims of the members of the class. Plaintiffs and all members of the class were damaged by the same wrongful conduct by CIQ and by LG (or an equivalent manufacturer, e.g. HTC, playing the same corporate-customer and informational role), *i.e.,* they all have had their devices and information unknowingly compromised as a result of Defendants' wrongful conduct.

42. Plaintiffs will fairly and adequately protect the interests of other class members because they have no interest that is antagonistic to or which conflicts with those of any other class member, and Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel experienced in litigation of this nature to represent Plaintiffs and other members of the class.

43. The prosecution of separate actions by individual members of the class would create the risk of inconsistent or varying adjudications with respect to individual members of the class, which could establish incompatible standards of conduct for Defendants.

44. This class action is the superior method for the fair and efficient adjudication of this controversy. Class treatment will permit a large number of similarly-situated individuals to prosecute their claims in a single forum simultaneously, efficiently and without the

unnecessary duplication of evidence, effort and expense that numerous individual actions would produce. The damages sustained by individual class members, although substantial, do not rise to the level where they would have a significant interest in controlling the prosecution of separate actions against these well-financed Defendants.

45. This case will be eminently manageable as a class action. Plaintiffs know of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

CAUSE OF ACTION

COUNT I – Violation of the Federal Wiretap Act as Amended by the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et. seq.

46. Plaintiffs incorporate the paragraphs above by reference as if fully set forth herein.

47. Plaintiffs bring this count against Carrier IQ on behalf of the Class, and against LG on behalf of the LG Subclass.

48. Defendants' actions as described herein violated the Federal Wiretap Act as Amended by the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et. seq. *See* 18 U.S.C. § 2511(1), 18 U.S.C. § 2520.

49. Defendants CIQ and LG, by way of the CIQ software and their own implementing or ancillary software, have intentionally intercepted, endeavored to intercept, or procured others to intercept or endeavor to intercept, wire and/or electronic communications as described herein, all without the knowledge, consent or authorization of Plaintiffs or the Class, in violation of 18 U.S.C. § 2511(1). *See* 18 U.S.C. § 2511(1)(a).

50. Defendants CIQ and LG, by way of the CIQ software and their own implementing or ancillary software, have intentionally disclosed, or endeavored to disclose, to other persons the contents of wire and/or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications, as described in 18 U.S.C. § 2511(1)(c).

51. Defendants used or endeavored to use the contents of the electronic communications of Plaintiffs and the Class, knowing and having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511 (1)(d).

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

53. Plaintiffs seek all appropriate relief on behalf of themselves and the proposed Class, including but not limited to statutory damages provided by 18 U.S.C. § 2520.

JURY TRIAL DEMAND

54. Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs, on their own behalves and on behalf of the class, demand a trial by jury of all claims asserted in this Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request entry of judgment against Defendants, jointly and severally:

a. Certifying that this action may be maintained as a class action under Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure, appointing Plaintiffs as class representatives and their counsel as lead class counsel;

b. Directing that reasonable notice of this action, as provided by Rule 23(c)(2) of the Federal Rules of Civil Procedure be given to members of the Class;

c. Awarding Plaintiffs and the Class their full monetary damages to be proven at trial;

d. Awarding Plaintiffs and the Class their statutory damages, pursuant to the Federal Wiretap Act as Amended by the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et. seq.;

e. Awarding Plaintiffs and the Class pre-and post-judgment interest on their damages;

f. Awarding Plaintiffs and the Class the costs of this action and reasonable attorneys' fees pursuant;

g. Enjoining Defendants from continuing or resuming their unlawful practices;

h. Awarding all other legal or equitable relief as appropriate to effectuate the purposes of the laws as referenced above; and

i. Awarding Plaintiffs and the Class such other and further relief as the Court deems just and proper.

Dated: December 6, 2011

Daniel L. Low (dlow@kotchen.com)
Kotchen & Low LLP

Of Counsel:

Daniel A. Kotchen (dkotchen@kotchen.com)
Robert Klinck (rklinck@kotchen.com)
Justin Ervin (jervin@kotchen.com)
Kotchen & Low LLP
2300 M Street, NW
Suite 800
Washington, D.C. 20037
(202) 416-1848
(202) 280-1128 (fax)

Michael F. Brown (mbrown@pbclaw.com)
Peterson, Berk & Cross, S.C.
200 E. College Ave.
Appleton, WI 54912
920-831-0300
920-831-0165 (fax)