LIONEL Z. GLANCY (#134180)
MARC L. GODINO (#182689)
GLANCY BINKOW & GOLDBERG LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
E-mail: info@glancylaw.com

MARC I. GROSS
JASON S. COWART
MATTHEW L. TUCCILLO
POMERANTZ HAUDEK
GROSSMAN & GROSS LLP
100 Park Avenue, 26th Floor
New York, New York 10017
Telephone: 212-661-1100
Facsimile: 212-661-8665
E-mail: mltuccillo@pomlaw.com

Counsel for Plaintiff Peter Medine
[Additional Counsel on Signature Page]

PSG

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CV11-06178

PETER MEDINE, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

CARRIER IQ, INC., AT&T INC., and APPLE, INC.,

Defendants.

Civil Action No. _____

JURY DEMAND

CLASS ACTION COMPLAINT FOR:

1. Violation of Federal Wiretap Act, 18 U.S.C. § 2511; AND
2. Violation of Stored Electronic Communica-tion Act,18 U.S.C. § 2701; AND
3. Violation of Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030; AND
4. Violation of Unfair Competition Law, Cal. Bus. & Prof. Code §§17200, et seq.; AND
5. Violation of Privacy Act, Cal. Gen. Laws Ch. 214 §1B; AND
6. Violation of the Common Law for Trespass to chattel; AND
7. Violation of the California Penal Code §§ 631 and 632.7.

CLASS ACTION COMPLAINT

Plaintiff Peter Medine ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his undersigned counsel, upon knowledge as to himself and otherwise upon information and belief, alleges as follows:

THE PARTIES

1. Plaintiff Peter Medine is an adult domiciled in San Francisco, California. Mr. Medine is an AT&T customer who owns and uses an Apple iPhone 4.

2. Defendant Carrier IQ is a California corporation based in Mountain View, CA. Carrier IQ designed and sells the rootkit software at issue in this case.

3. Defendant AT&T is a Delaware corporation based in Dallas, TX.

4. Defendant Apple, Inc. is a California corporation based in Cupertino, CA.

JURISDICTION AND VENUE

5. This court has personal jurisdiction because all Defendants are licensed to do business in the state of California and conduct business in and otherwise have sufficient contacts in this District.

6. This Court has subject matter jurisdiction over this action and Defendants pursuant to 28 U.S.C. § 1331 because this action arises under federal statutes, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the "Wiretap Act"), the Stored Electronic Communication Act, 18 U.S.C. § 2701 ("SECA") and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CAFA") and pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. §1367.

7. Venue is proper in this District because Defendants Carrier IQ and Apple maintain their principal executive offices and headquarters in this District, and a substantial part of the events giving rise to the claim occurred in this District.

SUBSTANTIVE ALLEGATIONS

8. This is a class action lawsuit brought on behalf of similarly situated persons who have or had a wireless contract Defendant AT&T Inc. ("AT&T"), who own or owned at least one device manufactured and/or distributed by Defendant Apple, Inc. ("Apple") which contained so-called "rootkit" software designed and sold by Defendant Carrier IQ, Inc. ("Carrier IQ"), during applicable limitations periods, and whose privacy was violated.

9. Carrier IQ, established in 2005, develops software that it, wireless service providers ("carriers"), and original equipment manufacturers ("OEMs") use to collect and intercept data and communications sent or received by a wide variety of electronic devices, including without limitation smartphones, tablets, and e-readers. Each of these devices includes an operating system, which is software consisting of programs and data that run on the devices and manage hardware and application software.

10. Carrier IQ sells rootkit software ostensibly designed to help carriers and OEMs identify and diagnose service and quality-related problems such as dropped calls and battery drain. A rookit software is one that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. Carrier IQ claims to be the market leader in sales of "mobile service intelligence" rootkit software.

11. The Carrier IQ software is, by the company's admission, currently installed on 150 million phones worldwide, mostly in the U.S. Notably, it is embedded by device

manufacturers, along with other software, prior to shipment of the devices.

12. Defendant Apple pre-installs Carrier IQ software on devices used by its customers on the AT&T network.

13. Last month, Connecticut-based technology blogger and app designer Trevor Eckhart "("Eckhart") reported that the Carrier IQ software is far less benign and does far more tracking than previously advertised. His post, available at http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/, stated:

> Carrier IQ is able to query any metric from a device. A metric can be a dropped call because of lack of service. The scope of the word metric is very broad though, including device type, such as manufacturer and model, available memory and battery life, the type of applications resident on the device, the geographical location of the device, the end user's pressing of keys on the device, usage history of the device, including those that characterize a user's interaction with a device. (From http://www.faqs.org/patents/app/20110106942).

14. As Eckhart discovered, a litany of "triggers" cause the Carrier IQ rookit software to collect data metrics. Moreover, while the metric collected could be an aggregated one, such as the devices that experienced a dropped call in California at 5 p.m. on a given day, the Carrier IQ software can be used to track far more specific, personal data from a single individual's device. As reported by Eckhart:

> 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.

15. Notably, Eckhart's findings are based in part on training materials posted on Carrier IQ's website, which Eckhart mirrored and posted so that others could independently verify his conclusions without fear that Carrier IQ would remove the information from its site.

16. Carrier IQ initially attacked Eckhart, firing off a cease and desist letter and accusing him of copyright infringement (for posting the training materials, which it removed from its website) and false statements and threatening him with six figure damages.

17. However, the Electronic Frontier Foundation ("EFF") defended Eckhart, and, on November 23, 2011, Carrier IQ retracted its letter, issuing a statement that read: "Our action was misguided and we are deeply sorry for any concern or trouble that our letter may have caused Mr. Eckhart." At the same time, Carrier IQ also stated:

> 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.

18. Eckhart next posted a Youtube video (available here: http://www.youtube.com/watch?feature=player_embedded&v=T17XQI_AYNo) demonstrating that – even when his device was not connected to any carrier's cellular site – the Carrier IQ software was secretly running on his device and, among other things, logging his individual keystrokes, the numbers he presses to make telephone calls, the text messages he sends, and the URLs he visited, even from websites that use security encryption to prevent tracking. Each device button has a correlating "wkeycode" that is recorded by Carrier IQ's software. Moreover, each time a phone performs simple functions, like being turned on or off, that information is gathered as well.

19. Carrier IQ's software not only creates detailed logs that secretly store information within the device, thereby creating a significant hacking risk, it also transmits such

information to Carrier IQ's customers, including OEMs and carriers, and to Carrier IQ itself which stores such information at the company.

20. In the wake of Eckhart's analysis, Bryan Chafin, reporting for the *Mac Observer*, wrote:

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

21. Andy Greenberg, reporting for *Forbes*, wrote:

> As Eckhart's analysis of the company's training videos and the debugging logs on his own HTC Evo handset have shown, Carrier IQ captures every keystroke on a device as well as location and other data, and potentially makes that data available to Carrier IQ's customers. The video he's created (below) shows every keystroke being sent to the highly-obscured application on the phone before a call, text message, or Internet data packet is ever communicated beyond the phone. Eckhart has found the application on Samsung, HTC, Nokia and RIM devices, and Carrier IQ claims on its website that it has installed the program on more than 140 million handsets.

22. Russell Holly, reporting for Geek.com, wrote:

> Eckhart put together a video of him turning on an HTC Ev03D with a completely stock (provided by HTC) ROM. He demonstrates that nowhere in the startup does any mention of CarrierIQ. There's nothing indicating that this software exists on the phone. When the applications are discovered, the ability to shut the apps down the same way you would any other app in Android has been circumvented. So, you now have a series of applications that you have to be extremely knowledgeable to find, and when you do find them they *cannot be turned off*. This is demonstrated in the first five minutes of the video, and these steps can be easily re-created if you have access to LogCat on your computer.
>
> When you receive a text, the video demonstrates that the CarrierIQ software is aware of the text message and its contents before the phone notifies you that you have a message. CarrierIQ and Sprint both were adamant that the body of an SMS was not recorded, and yet we can clearly see in the video that the text contents are read and tra.'lsmitted via the CarrierIQ applications. In an attempt to clear this matter up, I reached out to CarrierIQ again, who refused to comment and noted that they "are looking forwarding to our meeting with EFF this week and will continue to keep you updated."

> The video also demonstrates how this software records the keys that are pressed in the dialer, before a call is even made. Anytime you press a key in the dialer app, even if you just press random numbers and then close the application, that information is logged by CarrierIQ. If you place a call, that information is recorded as well, along with network strength values. This way if anything happens that would interrupt the call, your carrier can see why it happened and fix it. There's a real benefit to the CarrierIQ software, but it is clear that far more is being recorded than is necessary.
>
> This video has demonstrated a truly significant volume of information is being recorded. Passwords over HTTPS, the contents of your text messages, and plenty more are recorded and sent to the customers of CarrierIQ. A significant part of what was demonstrated is not included in any privacy agreement, and some of it was a direct contradiction of the statements that were made by these companies. It looks like we're being lied to, our information is being recorded, and there is nothing we can do about it.

23. As Eckhart illustrated, and has since been widely reported, Carrier IQ software is incredibly difficult for the average consumer to detect and nearly impossible to fully stop from operating consistently on the devices onto which it is installed. As explained by Wired, "The [Carrier IQ] software runs hidden from users, who generally can't find it or uninstall it without very sophisticated knowledge or by switching out the operating system by 'rooting' their phone and flashing an alternative operating system. While legal, rooting almost always voids a phone's warranty."

24. Another developer, Tim Schofield, extensively researched the presence of the Carrier IQ software on multiple Android smartphone platforms. Beyond the privacy issues, he observed that the embedded Carrier IQ software necessarily degrades the performance of any device on which it is installed. The software is *always operating and cannot be turned off.* It necessarily uses system resources, thus slowing device performance while decreasing battery life. As a result, because of the Carrier IQ software, in addition to having their private communications intercepted, Plaintiff and Class members are not getting the optimal

performance of the smartphone devices that they purchased, and which are marketed, in part, based on their speed, performance, and battery life.

25. CNN reported on December 1, 2011, that AT&T confirmed to CNN Money that handsets on its network run Carrier IQ's software and transmit information from it back to them. However, as Wired reported the next day, AT&T does not inform consumers how this information is used.

26. CNN also reported on December 1, 2011 that Apple confirmed to CNN Money that Carrier IQ software is running on some of its mobile devices, but said it stopped supporting the latest version of iOS and will completely eliminate Carrier IQ from all iPhones and iPads in the future. ARS Technica reported that Apple confirmed that iPhone 4 is still running Carrier IQ software.

27. Testing by a well-known iPhone hacker and blogger, Grant Paul, confirmed that Carrier IQ software existed on any iPhone that ran any version of iOS 3, iOS 4, and iOS 5 operating systems.

28. On December 2, 2011, Wired reported that Carrier IQ admitted that certain data is downloaded from devices once per day. Andrew Coward ("Coward"), Carrier IQ's Chief Marketing Officer, admitted to Wired that Carrier IQ is "seeing URLs and we can capture that information." Since Carrier IQ gets the URLs directly from the device, Wired reported that it is also table to record encrypted search terms employed on search engines (e.g. https://www.google.com/#hl=en&sugexp=ppwe&cp=3&gs_id=p&xhr=t&q=abortion+clinics) rather than merely the URL for the search engine itself (e.g. google.com). Coward told Wired, "We do recognize the power and value of this data. We're very aware that this information is

sensitive. It's a treasure trove." Coward also admitted to Wired that the data collected by Carrier IQ is linked to individual chip and phone identification numbers.

29. In truly alarming remarks made to CNN Money the same day, Coward expressed surprise at the information that Carrier IQ's software was tracking on individual devices. Coward stated, "We're as surprised as anybody to see all that information flowing. It raises a lot of questions for the industry – and not [only] for Carrier IQ."

30. The ramifications are tremendous. Christopher Soghoian, a cyberprivacy researcher and fellow at human rights organization Open Society called the information collected by Carrier IQ "a gold mine for a hacker" and a "huge issue" if transmitted to carriers.

31. Carriers do not disclose in their contracts the kind of tracking and surveillance that Carrier IQ's software performs, as demonstrated by Eckhart and as described *supra*. Moreover, without any disclosure of the intrusive and comprehensive nature of Carrier IQ's communication interception, data collection, and surveillance, Plaintiff and Class members were not capable of providing informed consent to Carrier IQ. Plaintiff and Class members reasonably expected that text messages, emails, and Internet browsing habits were private and confidential. They did not expect or have knowledge that Carrier IQ would illegally track, log, and transmit their private communications, much less share them with Carrier IQ's customers.

32. Carrier IQ does not enter into any agreement with device users, nor does it obtain their consent to store its software on their devices or to use

33. On November 30, 2011, The United States Senate Committee on the Judiciary wrote a letter to Carrier IQ, expressing deep concern about the scandal. Demanding immediate responses to 11 questions, the letter says that the actions alleged "may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse

Act. This is a potentially very serious matter." In addition, State Attorneys General have made inquiries with Carrier IQ, and European regulators have opened investigations.

34. The Electronic Privacy Information Center, a non-profit organization in Washington, D.C., noted that the use of Carrier IQ's software to log data may constitute an "unlawful intercept."

35. Carrier IQ's software is surreptitiously tracking, logging, and transmitting extraordinarily sensitive information from consumers' phones to the mobile phone carriers, without the knowledge or consent of the users, in violation of federal privacy laws. Defendants' willful and knowing actions violated the Federal Wiretap Act, the Stored Electronic Communication Act, and the Federal Computer Fraud and Abuse Act. The Plaintiff seeks damages and injunctive relief under these statutes on behalf of the entire Class for these violations.

CLASS ACTION ALLEGATIONS

36. Plaintiff brings this action both individually and as a class action pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3) against Defendants, on his own behalf and on the behalf of any person who owns a device in which Carrier IQ software was or is installed in the United States.

37. Members of the Class are so numerous that joinder of all members would be impracticable. Plaintiff estimates that there are more than 150 million members of the Class.

38. There are questions of law and fact common to all the members of the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendants installed Carrier IQ on Plaintiff's and Class members' devices without their knowledge or consent;

b. Whether Defendants used Carrier IQ's software to track, log, transmit, and/or store Plaintiff and Class members' electronic communications;

c. Whether such conduct was intentional;

d. Whether such conduct occurred without Plaintiff's and Class members' consent;

e. Whether Defendants obtained and continues to retain valuable, personal and/or private information from Class members;

f. Whether, because of Defendant's misconduct, Plaintiff and other Class members are entitled to damages, restitution, equitable relief, injunctive relief, or other relief, and the amount and nature of such relief.

39. The claims of Plaintiff are typical of the claims of the members of the Class. Plaintiff has no interests antagonistic to those of the Class, and Carrier IQ has no defenses unique to the Plaintiff.

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

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

a. The prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that would, as a practical matter, be dispositive of the interests of the other members not parties to the adjudications, or substantially impair or impede their ability to protect their interests;

b. The prosecution of separate actions by the members of the Class would create a risk of inconsistent or varying adjudications with respect to the

individual members of the Class, which would establish incompatible standards of conduct for Defendants;

c. Defendants acted or refused to act on grounds generally applicable to the Class; and

d. Questions of law and fact common to members of the Class predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

42. Plaintiff does not anticipate any difficulty in the management of this litigation.

COUNT I

VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2511

43. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

44. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the willful interception of any wire, oral, or electronic communication.

45. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

46. Defendants placed rootkit software on Plaintiff's and the Class members' phones that intercepted records of users' phone communications.

47. Neither the Plaintiff nor members of the Class consented to or were aware that the Defendants were violating federal law and tracking this information.

48. The data that the Defendants knowingly intercepted are "communications" within the meaning of the Wiretap Act.

49. Defendants intentionally and willfully placed the software on Plaintiff's and Class members' devices and intentionally and willfully intercepted the electronic communications of such users.

50. Plaintiff and Class members are persons whose electronic communications were intercepted within the meaning of Section 2520.

51. Section 2520 provides for preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and disgorgement of any profits earned by Defendants as a result of the above-described violations.

COUNT II

VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT, 18 U.S.C. § 2701

52. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

53. The Stored Electronic Communications Act ("SECA") provides a cause of action against a person who intentionally accesses without authorization a facility through which an electronic communication service is provided, or who intentionally exceeds an authorization to access that facility, and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in storage in such a system.

54. "Electronic Storage" is defined in the statute to be "any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof."

55. Defendants intentionally placed software on Plaintiff's and Class members' phones that accessed their stored electronic communications without authorization, and thus violated SECA.

56. Plaintiff and other members of the Class were harmed by Defendants' violations, and are entitled to statutory, actual and compensatory damages, injunctive relief, punitive damages, and reasonable attorneys' fees.

COUNT III

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030

57. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

58. Defendants intentionally accessed computers used by Plaintiff and Class members for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, and by obtaining information from such a protected computer.

59. Defendants knowingly caused the transmission of a program, information, code or command and as a result caused a loss to Plaintiff and Class members during any one-year period of at least $5,000 in the aggregate.

60. Plaintiff and the Class members have also suffered a violation of the right of privacy as a result of Defendants' knowing actions.

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

62. Plaintiff's and Class members' devices are "computers" within the meaning of the Act.

63. Defendants' unlawful access to Plaintiff's and Class members' computers and communications have caused irreparable injury. Unless restrained and enjoined, Defendant may continue to commit such acts. If Plaintiff's and Class members' remedies at law are not

adequate to compensate for these inflicted and threatened injuries, Plaintiff and the Class members are entitled to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

COUNT IV
VIOLATION OF THE UNFAIR COMPETITION LAW

(CAL. BUS. & PROF. CODE §§ 17200 *ET SEQ.*)

64. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

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

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

67. Defendants engaged in "unlawful" business practices under the UCL because they violated the California Consumer Protection Against Spyware Act, Cal. Bus. & Prof. Code §§ 22947-22947.6, the Electronic Communications Privacy Act and California Invasion of Privacy Act. Defendants are therefore in violation of the "unlawful" prong of the UCL.

68. Defendants engaged in "fraudulent" business practices under the UCL because they secretly installed the Carrier IQ software on Plaintiffs' devices, failed to disclose that the Carrier IQ software was always operating on such devices, failed to disclose that the Carrier IQ software was capable of intercepting Plaintiffs' private communications and, in fact intercepted such communications, and failed to disclosed that the Carrier IQ software degraded the performance and battery life of the devices on which it was installed. Defendants' omissions

and failures to disclose were "material" to Plaintiff and the class within the meaning of *In re Tobacco II Cases*, 46 Cal. 4th 298, 325 (Cal. 2009).

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

> ARTICLE I DECLARATION OF RIGHTS
>
> SECTION 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, ***and privacy***.

70. Defendants' business acts and practices are unfair because they cause harm and injury-in-fact to Plaintiff and Class Members. Defendants' conduct lacks reasonable and legitimate justification. Defendants have benefited from such conduct and practices, while Plaintiff and the Class Members have suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendants' conduct offends public policy in California tethered to the right of privacy set forth in the Constitution of the State of California, and California statutes recognizing the need for consumers to obtain material information with which they can take steps to safeguard their privacy interests.

71. Defendants' acts and practices were also fraudulent within the meaning of the DCL because they are likely to mislead the members of the public to whom they were directed.

72. By engaging in the acts and practices described herein, Defendants have committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiff and the Class have suffered injury-in-fact and have lost money and/or property-

specifically, personal confidential information and the full value of their Electronic Devices and personal confidential information.

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

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

75. As a result, Plaintiffs and the Class have suffered and will continue to suffer damages. Further, as a direct and proximate result of Defendant's willful and intentional actions, Plaintiffs and the Class have suffered damages in an amount to be determined at trial and, unless Defendant is restrained, Plaintiffs will continue to suffer damages.

COUNT V
VIOLATION OF THE PRIVACY ACT

(CAL. G.L. Ch. 214, §1B)

76. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

77. Defendant illegally intercepted, tracked, and recorded Plaintiff's and Class members' electronic communications as described herein.

78. Through the use of Carrier IQ's software, Defendants repeatedly disclosed to third parties and/or caused to be disclosed to third parties, Plaintiff's and Class members'

Internet browsing, search engine usage, text messaging, and telephone call information, which includes facts of a highly private, sensitive, personal or intimate nature.

79. Defendants did so knowing and intending to engage in conduct that Plaintiff and Class members did not reasonably expect, knowing that Plaintiff and Class members reasonably believed their privacy was protected, and knowing that their actions would seriously diminish, intrude upon, and invade Plaintiff's and Class members' privacy.

80. Defendants did so in a manner designed to evade detection and remediation by Plaintiff and Class Members.

81. Defendants had no legitimate, countervailing business interest in engaging in the conduct alleged herein.

82. Defendants' actions did unreasonably, substantially, and seriously interfere with Plaintiff's and Class members' privacy.

83. Defendants' actions did unreasonably, substantially, and seriously interfere with Plaintiff's and Class members' privacy.

84. Defendants' conduct has caused, and continues to cause, Plaintiff and Class Members irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's and Class members' remedy at law is not adequate to compensate them for these inflicted, imminent, threatened and continuing injuries, entitling Plaintiff and Class members to remedies including injunctive relief.

85. Plaintiff and Class members are entitled to equitable relief that includes Defendants' cessation of the illegal conduct alleged herein. Plaintiff and Class members are also entitled to equitable relief that includes an accounting of what personal information of

theirs was tracked, collected, logged, transmitted, used, merged and further disclosed to whom, under what circumstances, and for what purposes.

86. As a proximate and direct result of Defendants' invasion of privacy, Plaintiff and the Class members were harmed.

87. Plaintiff and the Class members are therefore entitled to damages in an amount to be determined at trial.

COUNT VI
TRESPASS TO CHATTEL

88. Plaintiff incorporates the above allegations by reference as if set forth more fully herein.

89. The common law prohibits the intentional intermeddling with personal property, including in this case Plaintiff's and Class members' devices, in the possession of another that results in the deprivation of the use of the personal property or the impairment of the condition, quality, or usefulness of the personal property, or that impairs some other legally protected interest, including the legally protected interest in privacy and confidential information.

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

91. Without Plaintiff and Class Members' authorization or consent, or in excess of any authorization or consent given, Defendants knowingly and intentionally accessed Plaintiff's and Class Members' property, thereby intermeddling with Plaintiff's and Class Members' right to exclusive possession of the property and causing injury to Plaintiff and the members of the Class.

92. Defendants engaged in deception and concealment to gain access to Plaintiff's and Class Members' computers.

93. Defendants engaged in the following conduct with respect to Plaintiff's and Class Members' devices: Defendants authorized and/or caused the installation of Carrier IQ's software on Plaintiff's and Class Members' devices; accessed and obtained control over Plaintiff's and Class Members' personal confidential information; and deliberately programmed the operation of Carrier IQ's software code to bypass and circumvent Plaintiff's and Class Members' device privacy and security controls, to remain beyond their detection and control, and to continue to function and operate without notice to or consent from them. All these acts were in excess of any authority Plaintiff and Class Members ever granted, and none were in legitimate furtherance of Plaintiff's and Class Members' use of their devices. By engaging in deception and misrepresentation, whatever authority or permission Plaintiff and Class Members may have granted to the Defendants did not apply to Defendants' conduct.

94. Defendants' installation and operation of its program used, interfered, and/or intermeddled with Plaintiff's and Class Members' devices. Such use, interference and/or intermeddling was without Plaintiff's and Class Members' consent or, in the alternative, in excess of Plaintiff's and Class Members' consent.

95. Defendants' installation and operation of its program constitutes trespass, nuisance, and an interference with Plaintiff's and Class Members' chattels, to wit, their devices and personal confidential information.

96. Defendants' installation and operation of Carrier IQ software impaired the condition and value of Plaintiff and Class Member's devices and compromised the integrity, condition and value of their personal confidential information.

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

98. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiff's and Class Members' property, Defendant has injured and impaired in the condition and value of Class Members' devices and personal confidential information, as follows:

a. by consuming the resources of and/or degrading the performance of Plaintiff's and Class Members' devices (including hard drive space, memory, processing cycles, Internet connectivity, and battery life);

b. by diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiff's and Class Members' devices;

c. by devaluing, interfering with, and/or diminishing Plaintiff's and Class Members' possessory interest in their devices and personal confidential information;

d. by altering and controlling the functioning of Plaintiff's and Class Members' devices and personal confidential information;

e. by infringing on Plaintiff's and Class Members' right to exclude others from their devices and personal confidential information;

f. by infringing on Plaintiff's and Class Members' right to determine, as owners of their devices, which programs should be installed and operating on them;

g. by compromising the integrity, security, and ownership of Plaintiff's and Class Members' devices and personal confidential information; and

h. by forcing Plaintiff and Class Members to expend money, time, and resources in order to attempt to identify and remove the Carrier IQ software installed on their devices without notice or consent.

99. Defendants' conduct constituted an ongoing and effectively permanent impairment of Plaintiff's and Class Members' devices and personal confidential information.

100. Plaintiff and Class Members each had and have legally protected, privacy and economic interests in their devices and personal confidential information.

101. Plaintiff and Class Members sustained harm as a result of Defendants' actions, in that the expected operation and use of their devices and personal confidential information were altered and diminished on an ongoing basis.

102. As a direct and proximate result of Defendants' trespass to chattels, interference, unauthorized access of and intermeddling with Plaintiff's and Class Members' Electronic Devices and personal confidential information, Plaintiff and Class Members have been injured, as described herein.

103. Plaintiff, individually and on behalf of the Class, seeks injunctive relief restraining Defendant from such further trespass to chattels and requiring Defendant to account

for its use of Plaintiff's and Class Members' devices and personal confidential information, account for the personal information they have acquired, purge such data, and pay damages in an amount to be determined.

COUNT VII

STATUTORY INVASION OF PRIVACY IN VIOLATION OF CALIFORNIA PENAL CODE §§ 631 AND 632.7

104. Plaintiff repeats and re-alleges each of the foregoing paragraphs as though fully set forth herein.

105. At all material times, Penal Code Sections 631 and 632.7 were in full force and effect and were binding upon Defendants, and existed for the benefit of the Class Members, including Plaintiff, all of whom are and/or were protected by the California Invasion of Privacy Act (penal Code §§ 630 *et seq).*

106. Plaintiff is informed, believes, and thereupon alleges that Defendants willfully and without the consent of all parties to communications, or in some other unauthorized manner, read, or attempted to read, or to learn the contents or meaning of messages, reports, or communications while the same were in transit or passing over wires, lines, or cables, or were being sent from, or received at any place within California; or used, or attempted to use, in some manner, or for any purpose, or to communicate in any way, any information so obtained, or aided, agreed with, employed, or conspired with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned herein during the Class Period. (Cal. 10 Pen.Code § 631(a).)

107. Plaintiff is further informed, believes, and thereupon alleges that Defendants, without the consent of all parties to the communication, intercepted or received and

intentionally recorded, or assisted in the interception or reception and intentional recordation of, a communication transmitted by and between the Electronic Devices. (Cal. Pen. Code § 632.7(a).)

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

1. Determine that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

2. Award compensatory damages, including statutory damages where available, in favor of Plaintiff and the other members of the Class against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

3. Permanently restrain Defendants, and their officers, agents, servants, employees and attorneys, from installing software on cell phones that could track the users' information in violation of federal law;

4. Award Plaintiff and the Class members their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

5. Grant Plaintiff such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

110. The Plaintiff demands a trial by jury of all issues so triable.

DATED: December 8, 2011

GLANCY BINKOW & GOLDBERG LLP

By: _____
Marc L. Godino
Lionel Z. Glancy
1801 Avenue of the Stars, Suite 311
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160

POMERANTZ HAUDEK
GROSSMAN & GROSS LLP

Marc I. Gross
Jason S. Cowart
Matthew L. Tuccillo
100 Park Avenue, 26th Floor
New York, New York 10017
Telephone: 212-661-1100
Facsimile: 212-661-8665

POMERANTZ HAUDEK
GROSSMAN & GROSS LLP

Patrick V. Dahlstrom
Leigh Handelman Smollar
Joshua B. Silverman
One North LaSalle Street, Suite 2225
Chicago, Illinois 60602

Telephone: 312-377-1181
Facsimile: 312-377-1184

Attorneys for Plaintiff