ORIGINAL

FILED
2011 DEC -5 A 11:15
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
N.D. CA-SAN JOSE

Paid
SC
99

IRA P. ROTHKEN (CA SBN 160029)
JARED R. SMITH (CA SBN 130343)
ROTHKEN LAW FIRM
3 Hamilton Landing, Suite 280
Novato, CA 94949
Telephone: (415) 924-4250
Facsimile: (415) 924-2905
Email: ira@techfirm.com
Email: jared@techfirm.com

JOHN R. PARKER, JR. (CA SBN 257761)
KERSHAW, CUTTER & RATINOFF, LLP
401 Watt Avenue
Sacramento, California 95864
Telephone: (916) 448-9800 (voice)
Facsimile: (916) 669-4499 (fax)
Email: jparker@kcrlegal.com

Counsel for Plaintiffs
JENNIFER SUE PATRICK and SCOTT LEWIS

E-filing

ADR

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

CV11-05842 PSG

BY FAX

JENNIFER SUE PATRICK, an individual and SCOTT LEWIS, an individual on Behalf of Themselves and for the Benefit of All with the Common or General Interest, Any Persons Injured, and All Others Similarly Situated,

Plaintiffs,

v.

CARRIER IQ, INC., a Delaware corporation and Does 1 to 100, inclusive

Defendants.

Civ. Action No.

CLASS ACTION

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

(1.) VIOLATION OF THE CALIFORNIA CONSUMER PROTECTION AGAINST COMPUTER SPYWARE ACT;
(2.) VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT;
(3.) VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT;
(4.) VIOLATION OF ARTICLE 1, SECTION 1 OF THE CALIFORNIA CONSTITUTION (PRIVACY);
(5.) VIOLATION OF CALIFORNIA PENAL CODE §§631 AND 637.2;
(6.) VIOLATION OF CAL. BUS. & PROF. CODE § 17200;

DEMAND FOR JURY TRIAL

Plaintiffs JENNIFER SUE PATRICK and SCOTT LEWIS (collectively, "Plaintiffs") brings this class action suit against CARRIER IQ, INC. ("CARRIER IQ" or "CIQ") and DOES 1 through 100, inclusive, (collectively "Defendants").

NATURE OF THE ACTION

1. Plaintiffs bring this class action suit on their own behalf and on behalf of all other owners of mobile devices containing the hidden Carrier IQ software ("Rootkit Software" or "Carrier IQ Software") nationwide, who were damaged as a result of the unauthorized privacy intrusion caused by operation of such software. This suit seeks to redress Defendant's interception of Plaintiffs' private data from their smartphone computing devices and storing such data on Defendant's servers without prior notification to or authorization by Plaintiffs.

2. Defendant's Rootkit Software is installed on numerous mobile devices nationwide including on information and belief the plaintiffs' mobile phones, and Defendant has failed to adequately inform or give notice to mobile phone owners including the Plaintiffs and proposed class regarding the presence of such Carrier IQ Software on mobile phones or function of the Rootkit Software or provide an opportunity to such consumers to provide consent to its implementation. As a result, without the knowledge or authorization of such consumers, including the plaintiffs and the proposed class, millions of users' private and sensitive data has been collected, transmitted to and stored by Defendant. In addition the Rootkit Software, on information and belief, is and has been consistently active on users smartphones including those of plaintiffs and the proposed class, using, without cell phone owner authorization, CPU cycles (reducing smartphone computer processor capacity), bandwidth, and storage space for which smartphone users' incurred damages and harm.

3. Andrew Coward, Carrier IQ's vice president for marketing, on information and belief, admitted that the company's Rootkit Software reports back amongst other things what consumer mobile phone applications are being used and what URLs or specific web pages are visited.

4. Rootkit Software manufactured by defendant is installed on mobile devices, including, but

not limited to, the "smartphone" cellular telephones of Plaintiffs JENNIFER SUE PATRICK and SCOTT LEWIS, along with the mobile devices of numerous other smartphone owners including those in the proposed class.

5. Carrier IQ's Rootkit Software on information and belief, unlawfully violates the privacy of consumers by various means, including means not yet presently known, but including known wrongful methods that intercept mobile phone users' data, including private and sensitive data that contains personally identifiable information, web sites and specific pages visited such as those which reveal highly sensitive healthcare, financial, and sexual content associated with and tethered to consumers including the plaintiffs and proposed class. Carrier IQ failed to obtain consumer notice and consent prior to installing the Rootkit Software or collecting and storing private data. Accordingly, Plaintiffs on behalf of themselves and proposed class seek damages and injunctive relief against defendants including Carrier IQ to stop the wrongful conduct.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from at least one Defendant; there are more than 100 Class members nationwide; and the aggregate amount in controversy exceeds $5 million. In addition this Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 in that Plaintiffs allege violations of Federal Law including the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 et seq. Furthermore the Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a).

7. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because Defendant Carrier IQ, Inc. is headquartered in this District and/or because the improper conduct alleged in this Complaint occurred primarily in, and was directed from, this District.

INTRADISTRICT ASSIGNMENT

8. Defendant CARRIER IQ, INC.'s principle executive offices and headquarters are located

in this District at 1200 Villa Street, Suite 200, Mountain View, CA 94041. Intra-district assignment to the Santa Clara Division in San Jose is proper pursuant to Local Civil Rule 3-2(d).

PARTIES

9. Plaintiff JENNIFER SUE PATRICK is a resident of the State of California and owner of a mobile device containing on information and belief Rootkit Software installed without her knowledge and consent.

10. Plaintiff SCOTT LEWIS is a resident of the State of California and owner of a mobile device containing on information and belief Rootkit Software installed without his knowledge and consent.

11. Defendant CARRIER IQ, INC., ("Carrier IQ" or "Defendant") is the provider of Rootkit Software installed in the mobile devices of Plaintiffs and was involved in the hidden installation of the Rootkit Software and interception of and storage of sensitive and private data without mobile phone users', including plaintiffs and proposed class, notice and consent. Defendant is a Delaware corporation headquartered in the State of California at 1200 Villa Street, Suite 200, Mountain View, CA 94041. Carrier IQ conducts business throughout the State of California and the nation.

12. Plaintiffs are unaware of the true names of DOES 1 through 100, who are individuals or entities who conspired with or aided and abetted CARRIER IQ or otherwise involved in and liable for the installation, use, and maintenance of the hidden Rootkit Software on Plaintiffs' and the proposed class' mobile devices and operating to intercept Plaintiffs' and proposed class' private and sensitive data without mobile phone user knowledge or consent. When the identity of these individuals or entities sued as Doe defendants are identified, Plaintiffs reserve the right to amend their complaint to name such parties in this Action to the extent feasible.

13. Defendant Carrier IQ, Inc. and DOES 1 through 100, acted both independently and jointly, in that they knowingly authorized, directed, ratified, approved, acquiesced, or

participated in the wrongful acts alleged in this Action by installing the hidden Rootkit Software on mobile devices and intercepting, using, and storing sensitive information, personal identifying information, personal information from Plaintiffs' and the proposed class' mobile devices without authority or consent of the Plaintiffs and the proposed class.

CLASS ACTION ALLEGATIONS

14. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of themselves and the following class:

> All persons or entities throughout the United States whose mobile devices contain or contained Carrier IQ software (the "Class").

15. The Class does not include Defendants or their officers, directors, or any entity in which Defendants hold a controlling interest.

16. **Numerosity**. The Class consists of at least hundreds of thousands of persons or entities, making joinder impracticable. CIQ has represented that its Carrier IQ Software is installed in over 140 million mobile devices.

17. **Typicality**. The claims of Plaintiffs are typical of the claims of all Class members. Plaintiffs and Class members were all subjected to Defendants' identical wrongful conduct based on the same transactions that occurred uniformly to the Class.

18. **Adequacy**. Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting class actions of this type. Plaintiffs and their counsel are committed to vigorously litigating this action, and have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

19. **Superiority**. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitive and would have no effective remedy. The class-wide treatment of common questions of law or fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiently of adjudication.

20. Defendants have acted or failed to act on grounds generally applicable to Plaintiffs and all Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class.

21. The factual and legal bases of Defendants' liability to all Class members are the same. All Class members have suffered harm as a result of Defendants' wrongdoing.

22. **Commonality**. There are many questions of law or fact common to the Class, and those questions predominate over any questions that may affect individual Class members. Common questions include but are not limited to the following:

a. Whether Defendants owed a duty to the Class to give notice of the existence and operation of Defendants' software on Plaintiffs' mobile devices and whether Defendants breached such duty;

b. Whether Defendants owed a duty to the Class to obtain authorization from owners and users of mobile devices to operate Defendants software on such devices for purposes of siphoning off information and transmitting and storing such information and whether Defendants breached such duty;

c. Whether Defendants' conduct violated the California Consumer Protection Against Computer Spyware Act;

d. Whether Defendants' conduct violated the Electronic Communications Privacy Act;

e. Whether Defendants' conduct violated the Computer Fraud and Abuse Act;

f. Whether Defendants' conduct was an invasion of privacy in violation of Article 1, Section 1 of the California Constitution;

g. Whether Defendants' conduct violated California Penal Code §§631 and 637.2;

h. Whether Defendants' conduct violated Cal. Bus. & Prof. Code § 17200;

i. Whether Plaintiffs and Class members have sustained damages, and if so, what is the proper measure of those damages and injunctive or equitable relief.

23. 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 all other

b. all or substantially all of the Web sites visited by the consumer, other than Web sites of the provider of the software,

29. Defendants installed the software in a manner designed to conceal from consumers the fact that the software was installed. Defendants on information and belief accessed or used the consumer's Internet service for the purpose of causing an authorized user, namely the plaintiffs and proposed class, to incur financial charges for bandwidth and related data services not authorized by such consumers. The Carrier IQ Software technology and its hidden nature prevented, without the authorization of an authorized user, through intentionally deceptive means, an authorized user's reasonable efforts to disable such software.

30. Defendants' conduct violated the CPACSA, causing damage to Plaintiffs.

31. Plaintiffs seek awards for statutory damages and any actual damages, punitive damages, court costs, attorney's fees, and any other relief the Court deems proper, for Defendants' violation of the CPACSA.

32. As a result of Defendants' violations of the CPACSA, Plaintiffs have suffered and are suffering irreparable injury. Unless restrained by this court, such injuries will continue to be inflicted. Plaintiffs seek injunctive relief as set forth herein.

SECOND CAUSE OF ACTION
(Violations of the Electronic Communications Privacy Act)

33. Plaintiffs re-allege all preceding allegations as if fully set forth herein and make the following allegations according to information available to them, which plaintiffs believe to be true.

34. The federal Electronic Communications Privacy Act of 1986 ("ECPA", at 18 U.S.C. § 2511(1) makes it unlawful for a person to "willfully intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 USC 2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of the ECPA.

35. The transmission of data by Plaintiffs and the Class between their mobile devices and the Internet constitute "electronic communications" within the meaning of 18 U.S.C. §2510.

36. Defendants have intentionally obtained and/or intercepted, by device or otherwise, plaintiffs' and class members' electronic communications without their knowledge, consent, or authorization and while such communications were still en route.

37. Defendants have intentionally used such electronic communications with knowledge or having reason to know that the electronic communications were obtained through interception for an unlawful purpose.

38. Defendants' intentional interception of these electronic communications without Plaintiffs' or Class members' knowledge, consent, or authorization was undertaken without a facially valid court order or certification.

39. Defendants exceeded their authorization to access and control private information concerning Plaintiffs' electronic communications, in violation of 18 U.S.C. § 2701.

40. Defendants unlawfully and knowingly divulged Plaintiffs' electronic communication contents and user information, in violation of 18 U.S.C. § 2702.

41. Defendants intentionally acquired and/or intercepted the contents of electronic communications sent by and/or received by Plaintiffs through the use of an electronic device.

42. Defendants intentionally acquired the communications that had been sent from or directed to Plaintiffs through their use of computers and other electronic devices which were part of, and utilized in, Defendants' electronic communications system, in violation of 18 U.S.C. § 2511 and pursuant to 18 U.S.C. § 2520.

43. Plaintiffs are "person[s] whose ... electronic communication is intercepted ... or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

44. According to information available to plaintiffs, which plaintiffs believe to be true, the activity of defendants is not activity which are necessary incidents to the rendition of their service or to protection of rights or property of any provider of that service, as might have been authorized pursuant to 18 U.S.C. § 2511(2).

45. Defendants are liable directly and/or vicariously violations of the ECPA. Plaintiffs therefore seek remedies authorized by 18 U.S.C. § 2520, including preliminary and permanent equitable and/or declaratory relief as may be appropriate, damages pursuant to subsection 2520(c), to be proven at trial, punitive damages, and reasonable attorney's fees and other litigation costs reasonably incurred.

46. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary, permanent, equitable and/or 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 Defendants' profits obtained from the above-described violations.

THIRD CAUSE OF ACTION
(Computer Fraud and Abuse Act (18 U.S.C. § 1030))

47. Plaintiffs re-allege all preceding allegations as if fully set forth herein.

48. By secretly installing software that records users' every keystroke and transmits data to Defendants, Defendants have accessed Plaintiffs' mobile devices, in the course of interstate commerce or communication, in excess of the authorization provided by Plaintiffs as described in the Computer Fraud and Abuse Act (the "Fraud Act") 18 U.S.C. § 1030(a)(2)(C).

49. Plaintiffs' mobile devices, and those of the Class, are protected computers pursuant to 18 U.S.C. § 1030(e)(2)(B).

50. Defendants further violated the Fraud Act by causing the transmission of information, the excessive use of plaintiffs and proposed class' consumer smartphone CPU cycles, storage space, and bandwidth, including for example Wi-Fi bandwidth, and as a result caused harm aggregating at least $5,000 in value.

51. Defendants' actions were knowing or reckless and, as described above, caused harm to Plaintiffs and proposed Class members.

52. Plaintiffs seek recovery for this loss, as well as injunctive and declaratory relief to prevent future harm.

FOURTH CAUSE OF ACTION

(Invasion of Privacy in Violation of Article 1, Section 1 of the California Constitution)

53. Plaintiffs re-allege all preceding allegations as if fully set forth herein.

54. Defendants have knowingly, recklessly or negligently disclosed, exploited, misappropriated and/or engaged in widespread commercial usage of private and sensitive information concerning Plaintiffs and the Class members for defendants' own benefit, without the knowledge or consent of Plaintiffs and the Class members. Defendants stockpiled private and sensitive information of Plaintiffs and the proposed class sufficient to paint a highly intrusive profile of such individuals. Such conduct constitutes a highly offensive and dangerous invasion of Class members' privacy in violation of the California Constitution.

55. As Plaintiffs and the Class members did not voluntarily disclose their personal and private information to defendants, such information was misappropriated by defendants. Plaintiffs and Class members provided such information without their knowledge it would be covertly monitored and disclosed to third parties, and they did not consent to having their personal and private information used for defendants' commercial gain.

56. As a result thereof, Plaintiffs and the Class members have been damaged by an amount according to proof at the time of trial and/or have been irreparably harmed by such conduct.

FIFTH CAUSE OF ACTION

(California Penal Code §§631 and 637.2)

57. Plaintiffs' re-allege all preceding allegations as if fully set forth herein.

58. In violation of California Penal Code §631, defendants, without the willful consent of Plaintiffs and the Class members, made an unauthorized connection to Plaintiffs' and Class members' mobile devices over the Internet in this State.

59. In violation of California Penal Code §631, defendants, without the willful consent of the Plaintiffs and Class members, attempted to use and did use and communicate, and did aid, agree and conspire to use, the information wrongfully obtained in violation of §631.

60. Pursuant to California Penal Code §637.2(c), which specifically states that actual damages or the threat of actual damages is not necessary to recover under this section, Plaintiffs and

each Class member is entitled to $5,000 or three times the actual damages sustained, whichever is greater.

61. Pursuant to California Penal Code §637.2(b), Plaintiffs and the Class members also request defendants' conduct alleged herein to be enjoined and restrained.

SIXTH CAUSE OF ACTION

(Unlawful, Unfair and Fraudulent Business Acts and Practices in Violation of California Business & Professions Code §17200 *et seq.*)

62. Plaintiffs' re-allege all preceding allegations as if fully set forth herein.

63. The acts, omissions, misrepresentations, practices and non-disclosures of defendants as alleged herein constituted unlawful, unfair and/or fraudulent business acts and practices and untrue and misleading advertising within the meaning of California Business & Professions Code §17200 *et seq.*

64. Defendants have engaged in "unlawful" business acts and practices by violating each of the statutes and laws alleged in the claims above including but not limited to the violation of the California Anti-Spyware statute, the California Constitutional Right to Privacy stated in Article 1, §1 of the California Constitution, the Federal ECPA, and the California Penal Code §§631 and 637.2.

65. Accordingly, defendants have violated California Business & Professions Code §17200's proscription against engaging in an "unlawful" business act or practice.

66. Plaintiffs reserve the right to allege other violations of law that constitutes unlawful business acts or practices. Such conduct is ongoing and continues to this date.

67. Defendants have also engaged in a "fraudulent" or deceptive business act or practice in that the representations, omissions, and non-disclosures of material facts described above have a likelihood to deceive Plaintiffs the Class and the general public – who unknowingly and without consent had malware installed and maintained on their smartphones and furthermore had confidential, private, and sensitive information covertly monitored, intercepted, transmitted, recorded and compiled by defendants.

68. Defendants have also engaged in an "unfair" business act or practice in that the harm

caused by the intercepting and disclosing of Plaintiffs', Class members' and the general public's personal and private information by defendants outweighs the utility of such conduct, and such conduct offends public policy, is immoral, unscrupulous, unethical, deceitful and offensive, or causes substantial injury to consumers.

69. The aforementioned unlawful, fraudulent or unfair business acts and practices conducted by defendants still continue to this day and present a threat to Plaintiffs, the Class members and the general public in that defendants have failed to publicly acknowledge the wrongfulness of their actions and to correct or publicly issue individual and comprehensive corrective notice to Plaintiffs, the Class and the general public accurately describing defendants' acts and practices, and provide full restitution and disgorgement of all.

70. Pursuant to California Business & Professions Code §17203, Plaintiffs, on behalf of themselves, the Class and/or the general public as appropriate, seek equitable relief from this Court as set forth in the Prayer for Relief, as appropriate.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment and relief against the defendants as follows:

a. Certifying the proposed Class under Fed. R. Civ. P. 23

b. Finding that Defendants are liable under all legal claims asserted herein for their failure to properly maintain the privacy of Class members' electronic information;

c. A temporary, preliminary or permanent order: (1) enjoining the defendants from conducting its business through the acts and practices described in this Complaint; (2) ordering the defendants to conduct a corrective advertising and information campaign accurately describing their business practices and, *inter alia*, advising consumers whose confidential data has already been disclosed how to prevent further unwanted intrusions; (3) ordering the off-site storage, destruction and/or purging of all personal and confidential information collected or shared as a result of defendants' wrongful conduct;

d. Awarding damages to the Class under the common law and statutory theories

alleged herein, including compensatory damages, consequential damages, punitive damages, and any other damages allowed under the law;

e. An order requiring defendants to provide such appropriate equitable monetary relief as may be necessary to restore any money or property, real or personal, to any person in interest which may have been acquired by such means of unfair competition and/or as may be necessary to prevent the use or employment of any practice which constitutes unfair competition, as the Court in its discretion deems appropriate and an order imposing an asset freeze or constructive trust on such monies;

f. Statutory damages, actual damages and/or punitive damages, as appropriate;

g. Pre- and post-judgment interest;

h. All costs, expenses, and attorneys fees including, but not limited to, attorneys' fees pursuant to, *inter alia*, California Code of Civil Procedure §1021.5; and

i. Awarding any other legal or equitable relief as justice requires as this Court may deem necessary, proper and/or appropriate

j. Plaintiffs requests that remediation be achieved through the payment of cy pres to organizations including, non-profit Internet privacy groups, to assist the General Public by helping to remedy past, present, and future privacy intrusions. (*See Kraus v. Trinity Management Services, Inc.* (2000) 23 Cal.4th 116)."

JURY DEMAND

Plaintiffs request a jury trial as to all issues triable by jury.

Respectfully submitted,

Dated: December 2, 2011

By: _____
IRA P. ROTHKEN

ROTHKEN LAW FIRM
3 Hamilton Landing, Suite 280
Novato, CA 94949
Tel: (415) 924-4250
Fax: (415) 924-2905
ira@techfirm.com

available methods for the fair and efficient adjudication of this controversy.

24. Injuries sustained by the Class flow from a common nucleus of operative facts. In each case where Defendants' software was installed on class members' mobile devices, class members were harmed when their keystroke and personal information was collected, transmitted and stored by Defendants without their knowledge, authorization or consent.

25. Class certification is appropriate under Fed. R. Civ. P. 23(a) and 23(b)(3). Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) with respect to the injunctive relief sought herein.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
(California Consumer Protection Against Computer Spyware Act, California Business & Professions Code § 22947, et seq. "CPACSA")

26. Plaintiffs re-allege all preceding allegations as if fully set forth herein. Carrier IQ is malware software that is deceptively or surreptitiously installed on consumer user computers namely in this Action smartphones by means of an intentional and material failure to provide any notice to an authorized user regarding the installation of software in order to deceive the consumer. Defendants are not authorized users of plaintiffs' mobile devices, as defined in Section 22947.1. On information and belief Defendants are using the Carrier IQ Software in a manner in excess of or in a manner unauthorized under Section 22947.3(d).

27. Defendants knew, consciously avoided actual knowledge, or willfully caused its software to be copied onto the mobile computing devices of consumers in the State of California, including Plaintiff and proposed class members.

28. On information and belief, defendants used the Carrier IQ Software to collect, through intentionally deceptive means, personally identifiable information, including, but not limited to:

a. through the use of a keystroke-logging function that records all keystrokes made by an authorized user who uses the computer and transfers that information from the computer to another person;