

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

RECEIVED & FILED
APR 03 2012
Sussex County SCP Division

Larry Sossin Pro Se

Plaintiff,

v.

GOOGLE INC.,

Defendant

Civil Action No.

JURY DEMAND

COMPLAINT FOR:

1. Violation of Federal Wiretap Act,
18 U.S.C. § 2511 AND
2. Violation of Stored Electronic Communication
Act, 18 U.S.C. § 2701; AND
3. Violation of Federal Computer Fraud and Abuse
Act, 18 U.S.C. § 1030

COMPLAINT

"Google Inc. and other advertising companies have been bypassing the privacy settings of millions of people using Apple Inc.'s Web browser on their iPhones and computers -tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked."

The Wall Street Journal, Feb. 16, 2012

Plaintiff Larry Sossin, on behalf of himself Pro Se, upon knowledge as to himself and otherwise upon information and belief, alleges as follows:

NATURE OF THE ACTION

1. This is a lawsuit brought by Plaintiff whose default privacy settings on the web browser software produced by Apple Inc. ("Apple"), known as "Safari," were knowingly circumvented by Google Inc. ("Google" or "Defendant") and whose privacy was violated.

2 As set forth below Plaintiff, suffered an invasion of his privacy, in direct violation of federal law, when Google developed and implemented a secret computer code to avoid the privacy default settings that had been designed by Apple to prevent advertisers and other third parties from secretly monitoring or tracking the web-browsing activities of Safari users. Google engaged in these illicit activities despite its express instruction that users of Apple's Safari needed to affirmatively disable the privacy protection function in order for tracking cookies to be installed on users' devices.

3. Google's 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 for these violations.

JURISDICTION AND VENUE

4. This Court has personal jurisdiction over the parties because Plaintiff is a resident of this District, and the Defendant continuously and systematically conducts business in New Jersey, and otherwise has minimum contacts with this State sufficient to establish personal jurisdiction over it.

5. This Court has subject matter jurisdiction over this action and Defendant 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 "CFAA") and pursuant to 28 U.S.C. § 1332(d) ("CAFA") because the amount in controversy exceeds \$5,000,000.

6. Venue is appropriately established in this court under 28 U.S.C 1391 (b)(2) because a substantial part of the events giving rise to the claim occurred in this district

THE PARTIES

7. Plaintiff is a resident of Sussex County in the State of New Jersey. Plaintiff uses Apple's Safari browser and never disabled the privacy protection within that software.

8. Defendant Google is a Delaware corporation based in Mountain View, CA.

FACTUAL BACKGROUND

9. Google describes itself as a "global technology leader focused on improving the ways people connect with information."

10. According to Google's most recent public filing on Form 10-K, Google "generate[s] revenue primarily by delivering relevant, cost-effective online advertising."

11. On or around February 16, 2012, *The Wall Street Journal* reported that Google has been "bypassing the privacy settings" of millions of people who use Apple's Safari software to browse the Internet and has been "tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked."

12. According to the article, Google uses a special computer code that "tricks Apple's Safari Web-browsing software" despite the fact that this software "is designed to block such tracking by default."

13. The article further explained that "[t]o get around Safari's default blocking, Google exploited a loophole in the browser's privacy settings" which excludes websites where "a person interacts in some way -for instance by filling out a form." As explained, "Google added coding to some of its ads that made Safari think that a person was submitting an invisible form to Google. Safari would then let Google install a cookie on the phone or computer." The

cookie (a small bit of code that is placed on a web browser to allow a user's web browsing activity to be monitored) then transmitted information on the user's web-browsing to Google's advertising network called "DoubleClick."

14. The Google code was first identified by a researcher at Stanford University and independently confirmed by *The Wall Street Journal's* own technical advisor.

15. The Electronic Frontier Foundation ("EFF"), a non-profit organization that promotes digital privacy rights on behalf of consumers and the general public, commented that as a result of Google's actions "users who want to be safe against web tracking can't rely on Safari's well-intentioned but circumventable protections." EFF explained that Google exploited "a small hole in Safari's privacy protections" but that this action "[u]nfortunately had the effect of completely undoing all of Safari's protections against doubleclick.net," the domain name to which Google would send personal information. EFF analogized that "[l]ike a balloon popped with a pinprick, all of Safari's protections against DoubleClick were gone."

16. EFF also noted that while Google was actively circumventing the Safari software, it was also advising its users, via its web page, that Safari has a default privacy protector that users must disable to allow web tracking: "While we don't yet have a Safari version of the Google advertising cookie opt-out plugin, Safari is set by default to block all third party cookies. If you have not changed those settings, this option effectively accomplished the same thing as setting the opt-out cookie." EFF lamented that "[i]f only that had stayed true" and concluded that "[a]ny code that was specifically designed to circumvent privacy protection features should have triggered a much higher level of review and caution, and that clearly did not happen."

17. Also on February 17, 2012, Washington, D.C.-based Consumer Watchdog sent a

take "immediate action" because Google had "violated people's online privacy choices and falsely advised them about how to make opt-out choices." The letter sites the above language from Google advising consumers that Safari's defaults must be altered by the user to permit cookies to be placed on the user's device, then complains that "the advice was false. Google was lying. It was in fact circumventing the privacy choice and setting DoubleClick tracking cookies." According to Consumer Watchdog, "[c]learly Google knows that it was wrong. After the company was confronted about the Stanford research, it changed its advice page, removing the specific references to Safari." The letter further complains that "Google's behavior is clearly 'unfair and deceptive'" and also violates the terms of a previous Consent Decree between Google and the FTC which states as follows:

It is ordered that respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication: (A) the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) The purposes for which it collects and uses information, and (2) the extent to which consumers may exercise control over collection, use, or disclosure of covered information.

18. According to Ars Technica ("Ars"), an Internet blog focusing on issues of technology, "[a]n Apple spokesperson told Ars that 'We are aware that some third parties are circumventing Safari's privacy features and we are working to put a stop to it.'"

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

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

26. The federal wiretap act , as ammended by the electronic communications privacy act of 1986, prohibits the willful interception of any wire, oral, or electronic communication.

27.27. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

28. Defendant circumvented the default privacy setting on Plaintiffs Safari browser and allowed a tracking cookie to be placed on Plaintiffs mobile phone or computer device.

29. Neither the Plaintiff nor members of the Class consented to or were aware that the Defendant was violating federal law and engaging in this activity.

30. The data that the Defendant knowingly intercepted are "communications" within the meaning of the Wiretap Act.

31. Defendant intentionally and willfully placed the tracking cookies on the mobile phones and computer devices of Plaintiff and members of the Class and willfully intercepted the electronic communications of such users.

32. Plaintiff is a person whose electronic communications were intercepted within the meaning of Section 2520.

33. 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 Defendant as a result of the above-described violations.

34.27. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

28. Defendant circumvented the default privacy setting on Plaintiffs Safari browser and allowed a tracking cookie to be placed on Plaintiffs mobile phone or computer device.

29. Neither the Plaintiff nor members of the Class consented to or were aware that the Defendant was violating federal law and engaging in this activity.

30. The data that the Defendant knowingly intercepted are "communications" within the meaning of the Wiretap Act.

31. Defendant intentionally and willfully placed the tracking cookies on the mobile phones and computer devices of Plaintiff and members of the Class and willfully intercepted the electronic communications of such users.

32. Plaintiff is a person whose electronic communications were intercepted within the meaning of Section 2520.

33. 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 Defendant as a result of the above-described violation

COUNT II

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

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

35. 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.

36. "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."

37. Defendant intentionally placed tracking cookies on the mobile phones and computer devices of Plaintiff and members of the Class and accessed their stored electronic communications without authorization, and thus violated SECA.

38. Plaintiff and other member of the Class were harmed by Defendant's 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

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

40. Defendant intentionally accessed a computer used 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.

41. Defendant knowingly caused the transmission of a program, information, code or command and as a result caused a loss to one or more persons during any one-year period of at least \$5,000 in the aggregate.

42. Plaintiff has also suffered a violation of the right of privacy as a result of Defendant's knowing actions.

43. Defendant has thus violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

44. Plaintiff's phone is a "computer" within the meaning of the Act.

45. Defendant's unlawful access to Plaintiff's computers and communications caused irreparable injury. Unless restrained and enjoined, Defendant may continue to commit such acts. If Plaintiff's remedies at law are not adequate to compensate for these inflicted and threatened injuries, Plaintiff and the Class are entitled to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully request that this Court:

A. Award compensatory damages, including statutory damages where available, in favor of Plaintiff For \$250,000.00 against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

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

D. Award Plaintiff reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

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

JURY TRIAL DEMAND

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

CERTIFICATION

Pursuant to L. Civ. R. 11.2, I hereby certify that the matter in controversy is not the subject of any other action pending, arbitration, or administrative proceeding to Plaintiffs knowledge.



4/2/12

Larry Sossin Pro Se
129 Idalroy trail
Hopatcong New Jersey 07843
(973) 713-3657

STAPLES copy&printcenter

Complimentary Self-Serve Fax Cover Sheet

To: Jeremy M. Klausner

Fax #: 201 408 5855

Date: 4/2/12

Number of Pages (Including Cover): 10

From: Larry Sossin

Phone #: 973 713 3657

Reply Fax #: _____

Urgent Confidential Confirm Receipt

We'll do it right the first time — guaranteed.

Black & white copies • Color copies • Custom printing • Binding • Folding • Wide-format copying • Custom stamps • UPS shipping and more



that was easy.