IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

NICHOLAS TODD HEINRICH,	**)**	
	)	
Plaintiff,	**)**	
	)	
v.	**)**	**Case No.**
	)	
GOOGLE, INC.,	**)**	**JURY DEMAND**
	)	
Defendant.	**)**	

CLASS ACTION COMPLAINT

Plaintiff Nicholas Todd Heinrich, for his Complaint against Google, Inc., states and alleges as follows:

INTRODUCTION

1. This action arises out of Defendant's intentional and secret efforts to evade the privacy settings in Apple's Safari browser software in order to access and track Safari users' Internet activities, so as to further Defendant's advertising business.

2. In this Complaint, Plaintiff seeks, on his own behalf and on behalf of a Class of all other users of Safari software, a judgment finding that Defendant Google, Inc. has violated federal and state law, and an award of statutory, compensatory and punitive damages and injunctive and other equitable relief, as well as attorneys' fees and costs, and such other and further relief as the Court deems appropriate.

PARTIES

3. Plaintiff is and has been at all relevant times a citizen and resident of Napa, California, uses Apple's Safari web browser on his Apple IPhone, and has not altered the default privacy settings in Safari. Upon information and belief, Defendant intercepted, collected, stored

and used Plaintiff’s private personal information for the purpose of misappropriating such information and unjustly enriching itself.

4. Defendant Google, Inc. is a Delaware corporation with headquarters in Mountain View, California. Google is a multi-national corporation specializing in internet search and advertising technologies. It describes itself as “a global technology leader focused on improving the ways people connect with information.” Google’s main source of revenue is advertising.

JURISDICTION AND VENUE

5. The claims in this Complaint arise in part under the federal Wiretap Act, 18 U.S.C. § 2511, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Stored Electronic Communications Act, 18 U.S.C. § 2701. As such, jurisdiction is proper in this Court pursuant to 28 U.S.C. § 1331.

6. Jurisdiction is also proper under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2).

7. Venue is proper in this District.

STATEMENT OF FACTS

8. Safari is a web browser included in all Apple IPhones, IPads, IPod Touches, and Mac computers. It includes “privacy settings” which allow a user to control the amount of information that is shared with advertisers and others and to control whether the user’s internet searches will be tracked or not.

9. Unlike most web browsers, the privacy settings in Safari by default enable blocking of “cookies,” small pieces of software placed on a computer to track the user’s Internet activities. In other words, all Apple products are sold to customers with this privacy setting turned on. In fact, Apple advertises this feature as one of the benefits of using Safari:

> Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from the current domain.

10. The purpose of this feature is to limit cookies from third party domains, that is, domains other than the first-party domain that appear in the browser's URL bar.

11. Thus, unless the user specifically authorizes it by changing the privacy settings, Safari will not allow a third party to install cookies, and so the third party will not be able to track the user's Internet activity.

12. Google itself acknowledged Safari's default settings, telling its users that it was sufficient to prevent 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.

13. Unbeknownst to users, however, Google surreptitiously implemented a program to evade these protections. As described by the Wall Street Journal, "Google and other advertising companies have been following IPhone and Apple users as they browse the web, even though Apple's Safari Web browser is set to block such tracking by default." *See* "How Google Tracked Safari Users," Wall Street Journal, Feb. 16, 2012. Thus, Google was able to "secretly track[ ] the Web-surfing habits of millions of people using the Safari browser on Apple's Mac computers, I Phones and I Pad tablets[.]" Chris Boulton, "Google Sued Over Safari Privacy Snafu," EWeek Mobile, Feb. 22, 2012 (available at Mobile.eweek.com/c/a/Security/Google-Sued-Over-Safari-Privacy-Snafu-395296/).

14. Google did so by exploiting a loophole in Safari's privacy settings. Although it blocks most tracking, Safari allows cookies from websites with which a user interacts, for

example, by filling out a form. According to the Wall Street Journal, Google tricked Safari into thinking a user had interacted, by "add[ing] code to some of its ads that made Safari think that person was submitting an invisible form to Google."

15. The Wall Street Journal described Google's efforts:

> To put cookies into Safari, Google's ads used something called an "iframe,' an invisible container that allows content from one website to be embedded within another site, such as an ad on a blog. [¶] Through this "iframe' window, Google received data from the user's browser and was able to tell whether the person was using Safari. If he was, Google then inserted an invisible form into the container. The user didn't see or fill out the form – in fact, there was nothing to "fill out" – but nevertheless, the Google code "submitted" it automatically. [¶] Once the form was sent, Safari behaved as though the user had filled something out intentionally, and the browser allowed Google to put a cookie on the user's machine.

16. Thus, Google, without the user's knowledge or consent, obtained "permission" from Safari to "track[ ] its users by allowing Google to install a cookie on a user's phone or computer without their consent or knowledge." Letter from Congressmen Edward J. Markey, Joe Barton, and Cliff Stearns to the Honorable Jon Leibowitz, Chairman of the Federal Trade Commission, February 17, 2012.

17. By doing so, according to Stanford researcher Jonathan Mayer, who discovered Google's secret, "all doubleclick.net content is now immunized from Safari's cookie blocking policy."

18. Quoting Mr. Mayer, the Wall Street Journal concluded, "'[t]here are zero legitimate-use cases' for advertisers to use an invisible form to enable tacking that Safari would have otherwise blocked."

19. As the Consumer Watchdog group concluded in a letter to the Federal Trade Commission Chairman dated February 17, 2012, "[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."

20. Moreover, Google's actions violated a Consent Decree entered into between Google and the FTC, to which Google agreed:

> 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.

CLASS ACTION ALLEGATIONS

21. Plaintiff brings this action on behalf of himself and a class of all persons similarly situated (the "Class members"). This action is properly maintainable as a class action pursuant to Fed. R. Civ. P. 23(a) and 23(b) (3).

22. The Class is defined as:

> All persons who used the Apple Safari Web browser and whose Safari default privacy settings Google altered, evaded or circumvented. Specifically excluded from the Class are the Court and of the Court's immediate family members, Defendant and its officers, directors, agents and employees.

23. The Class members are so numerous that joinder of all individual members in one action would be impracticable. The proposed Class includes millions of persons who use Apple's Safari Web browser.

24. Common questions of law and fact apply to the claims of all Class members, and those common questions predominate over questions that affect only individual Class members. The common questions include but are not limited to:

a. Whether Defendant intentionally altered, circumvented or evaded the default privacy settings in Apple's Safari Web browser;

b. Whether Defendant's conduct violated and continues to violate the federal Wiretap Act, the Computer Fraud and Abuse Act, and/or the Stored Electronic Communications Act;

c. Whether Defendant's conduct represents a trespass to Plaintiff's and the Class's personal property, an intrusion upon their seclusion, and/or whether Defendant was unjustly enriched;

d. Whether Defendant acted intentionally; and

e. Whether Plaintiff and Class members are entitled to recover statutory, compensatory and/or punitive damages, attorneys' fees and costs, or other injunctive and/or equitable relief based on Defendant's conduct.

25. Plaintiff's claims are typical of the claims of all Class members. Plaintiff and the other Class members were subjected to the same unlawful and intentional conduct by Defendant. The claims of Plaintiff and the other Class members are all based on the same legal theories.

26. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual actions are economically unfeasible and impractical.

27. Plaintiff will fairly and adequately represent and protect the interests of the Class members. Plaintiff has no interests that conflict with the interests of the other Class members. Plaintiff has retained qualified counsel, experienced in class actions, who will prosecute this action vigorously on behalf of the Class.

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

28. Plaintiff incorporates the preceding paragraphs as if fully set forth here.

29. The federal Wiretap Act, 18 U.S.C. § 2511(a), provides, in relevant part, that it is unlawful, except as otherwise specifically provided, for any person to "intentionally intercept[ ], endeavor[ ] to intercept, or procure[ ] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."

30. A private right of action is provided by 18 U.S.C. § 2520(a):

> Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

31. Section 2520(b) provides that in the event of a violation, “appropriate relief includes–

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

32. Section 2530(c)(2) provides that the Court “may assess as damages whichever is the greater of--

(A) The sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) Statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.”

31. The transmission of data between Plaintiff’s computer and the Internet constitutes “electronic communication” within the meaning of 18 U.S.C. § 2510(2).

32. Defendant’s data collection practices as described herein constitute “interceptions” within the meaning of 18 U.S.C. § 2510(4).

33. Defendant intentionally violated the Wiretap Act by installing and using software to evade the strictures of the default Safari Web browser privacy settings and by “intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to

intercept" the wire or electronic communication[s]" of Plaintiff and all other Class members in violation of 18 U.S.C. § 2511(a).

34. Defendant's actions as described herein were made without the consent of Apple or Plaintiff or the Class.

35. Defendant's actions as described herein were made for the purpose of committing tortious acts, in violation of federal and state law, including without limitation misappropriation of private and confidential information, unjust enrichment, intrusion upon the seclusion of Plaintiff and the Class, and trespass upon their personal property.

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

36. Plaintiff incorporates the preceding paragraphs as if fully set forth here.

37. 18 U.S.C. § 2707 provides a private cause of action to a person aggrieved by a violation of Section 2701 of the Stored Electronic Communications Act.

38. Section 2701 is violated when a person or entity:

> (1) Intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) 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 electronic storage in such system.

39. Plaintiff and the Class's computers are each a facility through which electronic communication service is provided.

40. Neither Plaintiff nor any Class member authorized Defendant to access information contained in the cookie Defendant implanted on Plaintiff's and Class members' computers.

41. Despite this lack of authorization, Defendant accessed private and confidential information electronically stored on Plaintiff's and Class members' computers.

42. As a result of Defendant's intentional and knowing violation of section 2701, and pursuant to 18 U.S.C. § 2707, Defendant is liable to Plaintiff and the Class for the sum of any actual damages they have suffered, as well as "any profits made by the [Defendant] as a result of the violation," with a minimum of $1,000 per person.

43. In addition, the Court may grant preliminary or other equitable or declaratory relief as appropriate, punitive damages for Defendant's willful or intentional misconduct, and Plaintiff's and the Class's attorneys' fees and costs of litigation.

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

44. Plaintiff incorporates the preceding paragraphs as if fully set forth here.

45. A person violates the Computer Fraud and Abuse Act by:

(a) Intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from a protected computer;

(b) Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and thereby furthers an intended fraud and obtains anything of value; or

(c) Knowingly caus[ing] transmission of a program, information, code or command and as a result causes damage without authorization, to a protected computer.

46. Plaintiff's and the Class's computers are each a "protected computer" within the meaning of 18 U.S.C. § 1030(e)(2) in that they are "used in or affecting interstate or foreign commerce or communication."

47. Neither Plaintiff nor any Class member authorized Defendant to exceed their authorized access to their computers or to use such access to obtain or alter information in their computer.

48. By reason of Defendant's misconduct, Plaintiff and Class members have been damaged within the meaning of 18 U.S.C. § 1030(8), in that Defendant impaired the integrity or availability of data, a program, a system, or information therein.

49. As a result of Defendant's misconduct, the Court should award Plaintiff and the Class compensatory damages, enter injunctive or other equitable relief as appropriate, and award Plaintiff and the Class their attorneys' fees and costs of litigation.

COUNT IV
UNJUST ENRICHMENT

50. Plaintiff incorporates the preceding paragraphs as if fully set forth here.

51. By means of Defendant's misconduct as described herein, Plaintiff and the Class conferred, without their consent, a benefit upon Defendant, that is, access to Plaintiff's and the Class's private and confidential information about their electronic communications over the Internet.

52. Upon information and belief, Defendant used that secretly and improperly procured information for commercial gain and so was unjustly enriched.

53. Defendant's retention of that commercial gain would be unjust and inequitable.

COUNT IV
TRESPASS TO PERSONAL PROPERTY

54. Plaintiff incorporates the preceding paragraphs as if fully set forth here.

55. Intentionally and without consent or other legal justification, Defendant placed cookies on Plaintiff's and the Class's computers and used those cookies to track Plaintiff's and the Class's Internet activities for purpose of commercial gain.

56. Defendant's surreptitious, intentional and unjustified placement of cookies on Plaintiff's and the Class's computers interfered with their use of their personal property, that is, their computers and their personally identifiable information.

COUNT IV
INTRUSION UPON SECLUSION

57. Plaintiff incorporates the preceding paragraphs as if fully set forth here.

58. By intercepting Plaintiff's and the Class's electronic communications, Defendant intentionally and deceptively intruded upon Plaintiff's and the Class's solitude and seclusion.

59. Defendant's intentional intrusion without consent would be highly offensive to a reasonable person.

WHEREFORE, Plaintiff prays that the Court enter judgment in favor of himself and the Class and against Defendant Google, Inc. as follows:

A. Determine that this case may properly be certified as a class action pursuant to Fed. R. Civ. P. 23 on behalf of a class as defined above;

B. Awarding Plaintiff and the Class statutory, compensatory and punitive damages;

C. Enjoining Defendant, its subsidiaries and agents to immediately cease and desist from surreptitiously attempting to evade the privacy settings in the Apple Safari web browser software and to eliminate any cookies or other software currently used to accomplish that evasion;

D. Awarding fees, expenses and costs to Plaintiff and his attorneys; and

F. Awarding such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands that all issues so triable in this Complaint be tried to a jury.

Nicholas Todd Heinrich

By: /s/ John R. Wylie
One of Plaintiff's attorneys

John R. Wylie
Charles R. Watkins
Donaldson & Guin LLC
300 South Wacker Drive, Suite 1700A
Chicago, Illinois 60606
Tel: 312-878-8391

David Guin
Tammy Stokes
Star M. Tyner
Donaldson & Guin LLC
The Financial Center
505 20th Street North, Suite 1000
Birmingham, Alabama 35203
Tel: 205-226-2282