

**FILED**

MAR - 6 2012

Clerk, U.S. District & Bankruptcy  
Courts for the District of Columbia

**UNITED STATES DISTRICT COURT  
DISTRICT OF COLUMBIA**

KEVIN JACOBSEN, On Behalf of  
Himself and All Others Similarly Situated,  
1301 20<sup>th</sup> Street NW  
Washington, D.C. 20036

Plaintiff,

vs.

GOOGLE, INC., a Delaware Corporation  
Registered Agent: The Corporation Trust Co.  
Corporation Trust Center  
1209 Orange Street  
Wilmington, DE 19801  
Defendant.

Case: 1:12-cv-00351  
Assigned To : Howell, Beryl A.  
Assign. Date : 3/6/2012  
Description: General Civil

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

**JURY  
ACTION**

Plaintiff, Kevin Jacobsen ("Plaintiff"), by and through his attorneys, hereby brings this Class Action Complaint on behalf of himself and all others similarly situated, and alleges as follows:

**INTRODUCTION**

1. Without disclosure to consumers, and without their permission, Defendant Google, Inc. inserted code into its web content that deactivated the security protections built into the Safari web browser and enabled tracking cookies to be installed on Safari users' computers, tablets, and smartphones.

2. This class action seeks to redress the violations of law arising from Defendant's surreptitious code. This lawsuit seeks damages for Plaintiff and the Class, including, but not limited to: damages and other available relief under the Federal Wiretap Act, the Computer Fraud and Abuse Act, and the Stored Electronics Communications Act; Plaintiff's attorneys' fees; and the costs of this lawsuit.

**JURISDICTION AND VENUE**

3. This Court has subject matter jurisdiction over this civil action under 28 U.S.C. § 1331, in that Plaintiff alleges violations of federal law, namely the Federal Wiretap Act as

amended by the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, and the Stored Electronics Communications Act, 18 U.S.C. § 2701 *et seq.*

4. Jurisdiction in this civil action is further authorized pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), as some Class Members' citizenship is diverse from Defendants, there are more than 100 putative Class Members, and the amount in controversy is in excess of \$5,000,000.

5. This Court has personal jurisdiction over the parties because Defendant conducts substantial business in the District of Columbia, has systematic and continuous contact with the District of Columbia, and has agents and representatives that can be found in the District of Columbia.

6. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), as a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

#### **PARTIES**

7. Plaintiff, Kevin Jacobsen, is a resident of the District of Columbia. Plaintiff owns a MacBook Pro, iPhone, and an iPad that all use the Safari web browser. Within the past year, Plaintiff has used these devices to use Google and view ads on various websites, including WashingtonPost.com new.evite.com, youtube.com, accuweather.com, cracked.com, quickmeme.com, and rottentomatoes.com.

8. Defendant Google, Inc. is a Delaware corporation, headquartered in Mountain View, California, with additional offices all over the world, including offices in Australia, Brazil, Canada, China, France, Germany, India, Ireland, Israel, Japan, Kenya, and the United Kingdom.

#### **FACTS**

9. Google describes itself as "a global technology leader focused on improving the ways people connect with information." *See* <http://investor.google.com/corporate/faq.html#toc-located>.

10. “Google primarily generates revenue by delivering relevant, cost-effective online advertising. Businesses use our AdWords program to promote their products and services with targeted advertising. In addition, third-parties that comprise our Google network use our Google AdSense program to deliver relevant ads that generate revenue and enhance the user experience.”

*Id.*

11. Through Google’s AdWords and AdSense programs, businesses and other third parties could have their ads displayed on various websites (hereinafter “Google Ads”).

12. Safari is an Internet web browser offered by Apple, Inc., that is pre-installed on iPhones, iPads, and Mac computers, and can be installed on PCs. To protect consumers’ privacy, Safari’s default settings block tracking the behavior of its users, which includes blocking third-party cookies.

13. Specifically, Safari’s defaults prohibit third parties such as advertising and web analytics firms from setting tracking “cookies”<sup>1</sup> without user authorization. This frustrated Defendant’s attempts to deliver personalized advertising and to enable full functionality of its products.

14. Stanford University researcher Jonathan Mayer discovered that Defendant inserted certain code into its products that circumvent Safari’s default privacy settings that block third-party cookies. By circumventing Safari’s default privacy settings, cookies can then be placed on Safari users’ devices and track the users’ browsing activity (“tracking cookies”).

---

<sup>1</sup> A “cookie” is “a small file or part of a file stored on a World Wide Web user’s computer, created and subsequently read by a Web site server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited).” *See* <http://www.merriam-webster.com/dictionary/cookies>.

15. This enabled Defendant to track users across the web even though their privacy settings said they did not want to be tracked.

16. Consumers' browsing activity has economic value. For example, Google's Screenwise program pays up to \$25 in gift cards for information on participants' web usage. *See* <http://www.google.com/landing/screenwisepanel/>.

17. Prior to the publication of Jonathan Mayer's research, Google provided browser instructions for Safari users: "Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the [Google advertising cookie opt-out plugin]."

18. This representation was false, as Google actively circumvented Safari privacy settings.

19. Google has since removed the above-quoted language from its webpage.

20. Google admits that it used code that was designed to ascertain whether Safari users were also signed in to Google and that, as a result of this code, tracking cookies could be, and were, placed on a Safari user's browser.

21. Within the past year, through his MacBook Pro, iPad and iPhone, Plaintiff has used Google and viewed ads on various websites, including WashingtonPost.com, new.evite.com, youtube.com, accuweather.com, cracked.com, quickmeme.com, and rottentomatoes.com. Plaintiff frequently visits such websites. On information and belief, visiting these websites and others allowed Defendant's tracking cookies to be placed on Plaintiff's devices without appropriate authorization and allowed Defendant to obtain, again without appropriate authorization, information pertaining to the websites that Plaintiff visited.

22. Google has begun to disable the concerned code after publication of Jonathan Mayer's research.

23. Nonetheless, upon information and belief it will require a time-consuming process to fully rid Plaintiff's devices of the unauthorized cookies, without also deleting the cookies that Plaintiff and Class Members have chosen to allow on their devices.

### **CLASS ACTION ALLEGATIONS**

24. Plaintiff brings this action on behalf of himself and additionally, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following Class:

All persons throughout the United States whose iPhone, iPad, Mac, or other device with Safari web browser installed on it, was subjected to the Google code that circumvented Safari's third-party cookie blocking feature and placed tracking cookies on their device(s) (the "Class").

25. Excluded from the Class is Defendant; any parent, subsidiary, or affiliate of Defendant; any entity in which Defendant has or had a controlling interest, or which Defendant otherwise controls or controlled; and any officer, director, employee, legal representative, predecessor, successor, or assignee of Defendant.

26. This action satisfies the requirements for class certification: numerosity, commonality, typicality, adequacy, predominance, and superiority.

27. This action has the requisite numerosity. The Safari web browser is installed on millions of devices and millions of Safari users have been affected. Thus, the Class consists of millions of persons. The Class is therefore so numerous that joinder of all members, whether otherwise required or permitted, is impracticable.

28. There are questions of law or fact common to the Class that predominate over any questions affecting only individual members, including, among others:

- a) Whether Defendant's code circumvents Safari's third-party cookie blocking feature;
- b) Whether the concerned code allows tracking cookies to be placed on Plaintiff's and Class Members' devices;
- c) Whether Defendant collects the browsing history of Plaintiff and Class Members through the concerned code and tracking cookies;

- e) Whether Defendant violated the Federal Wiretap Act;
- f) Whether Defendant violated the Computer Fraud and Abuse Act;
- g) Whether Defendant violated the Stored Electronic Communications Act;
- h) Whether Defendant has been unjustly enriched;
- i) Whether members of the Class have sustained damages and other compensable losses and, if so, the proper measure thereof; and
- j) Whether Class Members are entitled to statutory damages and other relief under the federal statutes and common law claim referenced herein.

29. The claims asserted by Plaintiff are typical of the claims of the members of the Class because they are similarly affected by the privacy-compromising code.

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

31. Predominance and superiority exist here for at least the following reasons:

- a) Absent a class action, members of the Class, as a practical matter, will be unable to obtain redress for Defendant's illegal conduct;
- b) It would be a substantial hardship for individual members of the Class if they were forced to prosecute individual actions;
- c) When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class;
- d) A class action will permit an orderly and expeditious administration of Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions;
- e) The lawsuit presents no difficulties that would impede its management by the Court as a class action;
- f) Defendant has acted on grounds generally applicable to members of the Class, making class-wide relief appropriate; and

- g) The prosecution of separate actions by individual members of the Class would create a risk of incompatible standards of conduct for Defendant and of inconsistent or varying adjudications for all parties.

**COUNT I**  
**FEDERAL WIRETAP ACT**

32. Plaintiff repeats and re-alleges the allegations contained in the paragraphs above, as if fully set forth herein.

33. Under the Federal Wiretap Act, it is unlawful 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.” 18 U.S.C. §2511 (a).

34. The Act also makes it unlawful for any person to disclose or use the contents of any electronic communication “knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.” 18 U.S.C. §2511 (c) and (d).

35. By placing code in Google Ads that circumvented Safari’s third-party cookie blocking feature, which allowed tracking cookies to be placed on Plaintiff’s devices and the devices of members of the Class, Defendants intentionally intercepted Plaintiff’s and Class members’ electronic communications and then used the communications, as the cookies track the users’ browsing history.

36. Statutory damages, punitive damages, reasonable attorneys’ fees, litigation costs reasonably incurred, and other appropriate relief is available in a civil action for any person whose electronic communication is intercepted, disclosed, or intentionally used in violation of the Act. 18 U.S.C. § 2520(b). The Court may assess statutory damages of “whichever is the greater of \$100 a day for each day of violation or \$10,000.” 18 U.S.C. § 2520(c)(2)(B).

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and the Class, requests that the Court enter judgment against Defendant as follows:

- A. Certifying the proposed Class under Federal Rule of Civil Procedure 23, and appointing Plaintiff and Plaintiff's counsel of record to represent the Class;
- B. Finding that Defendant has violated the Federal Wiretap Act, as alleged herein;
- C. Awarding Plaintiff and members of the Class statutory damages, punitive damages, and other appropriate relief (including the cost of removing the unauthorized cookies) against Defendants in an amount to be determined at trial;
- D. Awarding Plaintiff and members of the Class the reasonable costs and expenses of suit, including attorneys' fees; and
- E. Granting additional legal or equitable relief as this Court may find just and proper.

**COUNT II**  
**VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT**

37. Plaintiff repeats and re-alleges the allegations contained in the paragraphs above, as if fully set forth herein.

38. Under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, “the term ‘computer’ means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]” 18 U.S.C. § 1030(e)(1).

39. Under the Computer Fraud and Abuse Act, “the term ‘protected computer’ means a computer – . . . (B) which is used in or affecting interstate or foreign commerce or communication . . .” 18 U.S.C. § 1030(e)(2).

40. Plaintiff's devices fall within the definition of a protected computer, as they are used in interstate commerce or communication.

41. The Computer Fraud and Abuse Act makes it unlawful to intentionally access a computer without authorization, or to exceed authorized access, and thereby obtain information from any protected computer. 18 U.S.C. § 1030(a)(2)(C).



42. The “term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]”18 U.S.C. § 1030(e)(6).

43. The Computer Fraud and Abuse Act also makes it unlawful to intentionally access a computer without authorization and, as a result of such conduct, cause damage and loss. 18 U.S.C. § 1030(a)(5)(C).

44. The “term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information[.]”18 U.S.C. § 1030(e)(8).

45. The “term ‘loss’ means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]”18 U.S.C. § 1030(e)(11).

46. Plaintiff and members of the Class have suffered loss and economic damage as a result of Defendant’s tracking cookies, which allowed Defendant to access their web browsing activity that Defendant was not entitled to obtain.

47. A civil action may be brought by any person who suffers damage or loss by reason of a violation of the Computer Fraud and Abuse Act, provided that the conduct involves one of four factors set forth in subsection (c)(4)(A)(i) of the Act.

48. The aggregated loss to Plaintiff and members of the Class during the previous year exceeds \$5,000 in value. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and the Class, requests that the Court enter judgment against Defendant as follows:

A. Certifying the proposed Class under Federal Rule of Civil Procedure 23, and appointing Plaintiff and Plaintiff’s counsel of record to represent the Class;

B. Finding that Defendant has violated the Computer Fraud and Abuse Act, as alleged herein;

C. Awarding Plaintiff and Class Members economic damages (including the cost of removing the unauthorized cookies) as provided for under the Computer Fraud and Abuse Act, and other appropriate relief against Defendant in an amount to be determined at trial;

D. Awarding Plaintiff and Class Members the reasonable costs and expenses of suit, including attorneys' fees; and

E. Granting additional legal or equitable relief as this Court may find just and proper.

**COUNT III**  
**VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT**

49. Plaintiff repeats and re-alleges the allegations contained in the paragraphs above, as if fully set forth herein.

50. The Stored Electronic Communications Act, 18 U.S.C. § 2701 *et seq.*, makes it unlawful to intentionally access, without authorization or by exceeding authorization, a facility through which an electronic communication service is provided, and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system. 18 U.S.C. § 2701(a)(1)-(2).

51. Any person aggrieved by any violation of the Stored Electronics Communications Act, in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind, may recover from that entity appropriate relief, including:

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c); and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

18 U.S.C. § 2707(b).

52. Subsection (c) of the statute further provides that:

The court may assess as damages in a civil action under this section the

sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

18 U.S.C. § 2707(c).

53. Through its tracking cookies, Defendant intentionally accessed, without authorization or by exceeding its authorization, Plaintiff's and Class Members' computers and smartphones and obtained the users' online browsing activity while it was in electronic storage.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and the Class, requests that the Court enter judgment against Defendant as follows:

A. Certifying the proposed Class under Federal Rule of Civil Procedure 23, and appointing Plaintiff and Plaintiff's counsel of record to represent the Class;

B. Finding that Defendant has violated the Stored Electronic Communications Act, as alleged herein;

C. Awarding Plaintiff and members of the Class actual damages (including the costs of removing the unauthorized cookies), Defendant's profits, or the statutory minimum of \$1,000 per person, as provided for under the Stored Electronic Communications Act, and punitive damages and any other appropriate relief against Defendant in an amount to be determined at trial;

D. Awarding Plaintiff and members of the Class the reasonable costs and expenses of suit, including attorneys' fees; and

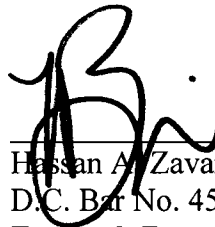
E. Granting additional legal or equitable relief as this Court may find just and proper.

**JURY TRIAL DEMANDED**

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

Dated: March 6, 2012

Respectfully Submitted,



---

Hassan A. Zavareei ✓  
D.C. Bar No. 456161  
TYCKO & ZAVAREEI LLP  
2000 L Street, NW, Suite 808  
Washington, D.C. 20036  
(202) 973-0900  
(202) 973-0950 (fax)  
hzavareei@tzlegal.com

*Counsel for Plaintiff  
and the Proposed Class*