

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA  
MIAMI DIVISION**

**KENNETH W. HERETICK,**  
individually, and on behalf of all others  
similarly situated,

**Plaintiffs,**

v.

**GOOGLE INC.,**

**Defendant.**

Case No.: \_\_\_\_\_ - CIV- \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff, Kenneth W. Heretick, individually and on behalf of all others similarly situated, through his attorneys, brings this class action Complaint against Defendant, Google Inc., and alleges:

**NATURE OF THE ACTION**

1. As permitted by Federal Rules of Civil Procedure 23(a), (b)(1), and (b)(3), Plaintiff brings this consumer class action lawsuit against the Defendant, Google Inc., on his own behalf and on behalf of a class of similarly situated users of the Apple® Safari® Internet web browser application (“Safari®”), all of whom were victims of unfair, deceptive, and unlawful business practices resulting from Google Inc.’s surreptitious and intentional circumvention of privacy controls of the Safari® web browser on Class Members’ mobile phones and other devices, such as the Apple® iPhone®, iPod Touch® and iPad®.

2. Mobile digital devices today are much more like desktop computers: many run complex operating systems and software applications to run specialized tasks. Unlike desktop computers, however, mobile digital devices are *uniquely mobile*, which introduces unique privacy implications for their owners. For the most part, mobile digital devices are “always on” devices, whose locations closely mirror that of their owners locations and activities. The historical location data can suggest trends that uniquely identify an individual mobile digital devices keep a local copy, or “cache” of location information from previous queries on the mobile digital device.<sup>1</sup>

3. A “cookie” is a small text file that a website sends to a visitor’s computer, where it is stored on the hard drive of an individual computer or mobile digital device, like web-enabled mobile digital devices such as the Apple® iPhone®. A cookie is generated by a web page server, which is basically the computer that operates a web site. The information the cookie contains is set by the server and it can be used by that server whenever the user visits the site. Depending on the information an Internet user enters on a site, data stored on a cookie may contain a number of user-specific, unique identifiers. Cookies enable web sites to monitor their users’ web surfing habits and profile them for marketing purposes (for example, to find out which products or services they are interested in and send them targeted advertisements). A cookie can be thought of as an internet user’s identification card, which tell a web site when the user has returned: they

---

<sup>1</sup> Oral and Written Testimony of Ashkan Soltani, Independent Privacy Researcher and Consultant, *Hearing on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy*, before the United States Senate, Judiciary Subcommittee on Privacy, Technology and the Law (May 10, 2011).

contain and transfer to the server as much information as the users themselves have disclosed to a certain web site.<sup>2</sup>

4. Permanent, persistent or stored cookies are stored on the user's computer or mobile digital device and are not deleted when the browser is closed. Permanent cookies can retain user preferences for a particular web site, allowing those preferences to be used in future browsing sessions. These types of cookies can be used to identify individual users, so they may be used by web sites to analyze users' surfing behavior within the web site. These cookies can also be used to provide information about numbers of visitors, the average time spent on a particular page and generally the performance of the web site. They are usually configured to keep track of users for a prolonged period of time, in some cases many years into the future.<sup>3</sup>

5. A server can only set a first-party cookie—that is a domain of which it a member. These are known as first-party cookies. In spite of this, users quite often find in their computer files cookies from web sites that they have never visited. These cookies are usually set by companies that sell internet advertising on behalf of other web sites, and are known as third-party cookies. In other words, first-party cookies are cookies set with the same domain (or its subdomain) in your browser's address bar. Third-party cookies are cookies being set with different domains than the one shown on the address bar (i.e. the web pages on that domain may feature content from a third-party domain. The most common reason people reject or fear cookies is their desire to avoid having information about their surfing habits is passed on to third-party web sites without the users' knowledge or consent.<sup>4</sup>

---

<sup>2</sup> Aboutcookies.org, *Cookies: Frequently Asked Questions, What is a Cookie?*, available at <http://www.aboutcookies.org/default.aspx?page=5> (last accessed February 20, 2012).

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

6. Publishers desiring to identify and track users while they are on their site embed first-party cookies. Third-party cookies allow companies to observe Internet browsing across many websites and acquire extensive behavioral data. The cumulative result of third-party tracking is that the cookies are placed on the user's hard drives without having visited a site or without having taken affirmative action to permit this invasion of privacy.

7. Defendant, Google Inc., historically operates most of its first-party websites on the "google.com" domain and most of its third-party services on other domains. For instance, Google Analytics™ web analytics service is served from "google-analytics.com" and its advertising services are on "doubleclick.net".<sup>5</sup> Typically, browsers that accept third-party cookies permit third-parties to set cookies from Defendant's "google.com" domain. Separating first-party websites from third-party services improves security: interactions between "google.com" content and that of other website could introduce vulnerabilities. The domain separation also benefits user privacy: Google Inc. associates user information with "google.com" cookies. By serving third-party services from other domains, companies protect third parties from receiving or identifying Google™ search engine user activities on other websites.<sup>6</sup>

8. Browser cookie controls and preference settings provide greater user privacy control. Browser privacy mode allows users to browse the Internet without leaving data tracks. Cookie controls allow the user to decide which cookies can be stored and transmitted. Blocking third party cookies can be difficult and prove frustrating to the user. But Apple® configures its

---

<sup>5</sup> *Id.*

<sup>6</sup> Johnathan Mayer, *Web Policy, Safari Trackers, Do Not Track, Measurement, Privacy* (Feb. 17, 2012), available at <http://webolicy.org/2012/02/17/safari-trackers/> (last accessed Feb. 18, 2012).

Safari® web browser to block third party cookies by default. Apple® markets its default cookie blocking as a benefit of choosing Safari.<sup>7</sup>

9. Defendant, Google Inc. intentionally created a code to operate as a work-around to the Safari® web browser's cookie blocking privacy protections that ultimately fooled the Plaintiffs' Safari® browsers into allowing otherwise blocked content to appear when Plaintiffs called up the Google™ search engine using a Safari® browser. To do this, Defendant used the code to use data it had already collected to make the Safari® browser think that *the user* of the mobile digital device was interacting with the web page by filling out a form. This permitted Defendant to install another cookie on the Plaintiffs' respective devices and track their browsing across the web on non-Google Inc. website. This practice let letting in the advertisers flow and tracking outgoing information flow, despite Plaintiffs' choices of browser privacy settings.

10. Defendant failed to adhere to its own comprehensive privacy program (the "Privacy Effort"), which is documented in written policies and procedures. Defendant ignored reasonably foreseeable, material risks, both internal and external, that resulted in order to engage in and profit from illegal tracking and recording of Plaintiffs' Internet presence, usage, movements, history, preferences, and locations, without Plaintiffs' knowledge or consent and irrespective of whether or not Plaintiffs were logged in as a Google+™ social service user or Gmail™ webmail service user.

---

<sup>7</sup> "Safari® is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from the current domain." Apple.com, *Safari Features, Security and Privacy, Cookie Blocking*, available at <http://www.apple.com/safari/features.html#security> (last accessed on February 19, 2012).

11. The conduct complained of includes, but is not limited to: Defendant's deliberate and intentional interference with privacy protections built into Plaintiffs' respective Safari® web browsers; Defendant's exercising wrongful interference, dominion, and control over Plaintiffs' computers and mobile digital devices without Plaintiffs' express or implied consent and in a manner inconsistent with their property, privacy, and security interests; Defendant's wrongful interference with and/or dispossession of Plaintiffs' personal property without their knowledge and consent; Defendant's interception in transit of Plaintiffs' electronic communications and embedding and storage of a persistent tracking cookie on Class Members' respective device hard drives, which intentionally circumvented the Safari® browser's cookie blocking feature; and Defendant's transmitting or causing Plaintiffs' computers or mobile digital devices to transmit data and intelligences over the Internet to deprive Plaintiffs of tangible and intangible personal property to obtain a benefit to which Defendant was not entitled.

12. Overriding privacy preferences and doing so without notice are unfair and deceptive business practices. Defendant's intentional acts and omissions resulted in one or more of the following:

- a. Violations of Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- b. Violations of Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522;
- c. Violations of Florida Deceptive and Unfair Trade Practices Act, §§ 501.201-501.213;
- d. Violations of Florida Communications Fraud Act, § 817.034;
- e. Trespass to Property (Chattels); and
- f. Unjust Enrichment/Restitution

13. Plaintiffs expressly reserve the right to supplement this Complaint as other information relevant to this action becomes available.

### **JURISDICITON AND VENUE**

14. Subject matter jurisdiction exists in this Court under 28 U.S.C. §§ 1331 because this action arises, in part, under federal law. This Court also has supplemental subject matter jurisdiction over the state law allegations raised in this Complaint exists in this Court as provided by 28 U.S.C. §§ 1367(a).

15. Venue is proper in this judicial district under 28 U.S.C. §1391 (b) and (c) because Defendant conducts and transacts substantial business in this judicial district, a substantial portion of the events and conduct giving rise to the violations complained of in this action occurred in this judicial district, and Defendant conducts business with consumers in this judicial district through its Google™ search engine and Safari® web browsers in use within this judicial district.

### **PARTIES**

16. Plaintiff, Kenneth W. Heretick (“Plaintiff”), is an adult citizen and current resident of Pinellas County, Florida. At all times relevant to this Complaint, Plaintiff used an Apple® iPad® mobile digital device (“iPad®”) and Apple® iPhone® (“iPhone®”)<sup>8</sup> to regularly access the Internet using the integrated Apple® Safari® web browser to access online content. Plaintiff did not change the default Safari® web browser privacy settings on his iPad® or iPhone® from which he regularly, if not exclusively, used the Google™ search engine to perform Internet searches or inquiries. Plaintiff relied on Google Inc.’s statements, privacy and security policies and believed Google Inc. would not track his Internet presence, usage, movements, history,

---

<sup>8</sup> Throughout this Complaint, Plaintiff’s personal iPad® and iPhone® as well as the general category of affected web-enabled devices referenced throughout are generally referred to as “computers and mobile digital devices”.

preferences, and locations using third-party cookies without permission. Plaintiff was injured when, without his consent, Google Inc. developed a code to exploit the default privacy settings on the integrated Safari® web browser on his iPad® and iPhone® in order to embed and record a permanent tracking cookies on and deliver unsolicited content to his iPad® iPhone®.

17. Defendant, Google Inc. is a Delaware Corporation, having its principal place of business in Mountain View, Santa Clara County, California. Google Inc. conducts substantial business throughout Florida and this judicial district through its Google™ search engine, Google+™ social service and other Google Inc. products.

### **CLASS ACTION ALLEGATIONS**

18. Plaintiff repeats and fully incorporates every allegation in ¶¶ 1-17.

19. Plaintiff brings this action on his own behalf and on behalf of the all others similarly situated as permitted by Federal Rules of Civil Procedure 23(a), (b)(1), and (b)(3). While the exact number of Class Members is unknown at this time, Plaintiff is informed and believes there are millions of members in the proposed class. The proposed class consists of:

**All persons in the United States who purchased or personally owned an Apple® iPhone®, iPod Touch®, or iPad® and used the integrated Apple® Safari® web browser to regularly access and use the Google™ search engine, Google+™ social service, and other Google Inc. under Google Inc.'s uniform privacy policies.**

20. The class is so numerous that joinder of all members is impracticable.

21. These actions involves questions of fact common to all Class Members because all Class Members used the Safari® web browser to regularly access and use the Google™



search engine, Google+™ social service, and other Google Inc. under Google Inc.'s uniform privacy policies.

22. This action involves common questions of law common to all Class Members including:

a. Whether Defendant's privacy invasions violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

b. Whether Defendant's privacy invasions violated the Communications Privacy Act, 18 U.S.C. §§ 2510-2522;

c. Whether Defendant's privacy invasions violated the Florida Deceptive and Unfair Trade Practices Act, §§ 501.201-501.213;

d. Whether Defendant's privacy invasions violated the Florida Communications Fraud Act, § 817.034; and

e. Whether Defendant's privacy invasions violated Plaintiff's and Class Members' common law and equitable rights in uniform ways.

f. The relief, including damages and equitable relief, to which Plaintiff and Class members are entitled.

23. Plaintiff will fairly and adequately protect the interests of the class.

24. Plaintiff's claims are typical of those of other Class Members as there are no material differences in the facts and law underlying their claims and Plaintiff's prosecution of their claims will advance the claims of all Class Members.

25. Plaintiff has retained competent counsel experienced in the prosecution of this type of class litigation.

26. The common question of law and fact among all Class Members predominate over any issues affecting individual Class Members, which include, but are not limited to:

a. Whether Defendant developed a code intended to exploit and bypass Safari® web browser's cookie blocking feature to intercept in transit Class Members' electronic communications, embed, and store a persistent tracking cookie on Class Members' respective device hard drives.

b. Whether Defendant intentionally circumvented the Safari® web browser's privacy protections on Class Members' personal computers, mobile phones, and other devices without their knowledge and express or implied consent in order to engage in online behavioral monitoring, analytics, and targeted marketing from which Defendant profited;

c. Whether Defendant exercised wrongful interference, dominion, and control over Class Members' computers and mobile digital devices without Class Members' express or implied consent and in a manner inconsistent with their property, privacy, and security interests;

d. Whether Defendant wrongfully interfered with and/or dispossessed Class Members of their personal property without their knowledge and consent;

e. Whether Defendant failed to disclose material terms in its privacy policy regarding its alteration, circumvention, and exploitation the Safari® web browser's privacy protections to embed and record a permanent tracking cookie on Plaintiff and Class Member's computers and mobile digital devices for Defendant's financial gain;

f. Whether Defendant's conduct constitutes violations of the laws cited in this Complaint.

g. Whether Plaintiff and Class Members are entitled to injunctive and declaratory relief;

h. Whether Plaintiff and the Class Members have sustained monetary loss and the proper measure of that loss; and

i. Whether Plaintiff and the Class Members have sustained consequential loss, and, if so, to what measure.

27. Class treatment of the claims set forth in this Complaint is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for the proposed Class Members to prosecute their claims individually. Absent a class action, a multiplicity of individual lawsuits would be required to address the claims between the Class Members and the Defendant so that inconsistent treatment and adjudication of the claims would likely result.

28. The litigation and trial of Plaintiff's claims is manageable. Defendant's standardized Terms of Service at issue, uniform deployment of code and systems that track each user in identical ways, the consistent provisions of the relevant laws, and the readily ascertainable identities of many Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

29. Adequate notice can be given to Class Members directly using information maintained in Defendant's records or through publication.

30. Damages may be calculated from the information maintained in Defendant's records, so that the cost of administering a recovery for the Class Members can be minimized. The amount of damages can also be known with precision through Defendant's records or as more specifically defined by the laws cited in this Complaint.

31. Defendant has acted or refused to act on grounds that apply generally to the class so that final injunctive relief and corresponding declaratory relief are appropriate.

32. Unless a class-wide injunction is issued, Defendant may continue to commit violations alleged, and the members of the class will continue to be tracked, unlawfully surveyed, and endangered without their consent.

33. Defendant has acted or refused to act on grounds that apply generally to the class, making final injunctive relief appropriate to the class as a whole.

34. Defendant's acts and omissions are the direct and proximate cause of damage in described more fully in the succeeding paragraphs of this Complaint.

## **COUNT I**

### **Violations of Computer Fraud and Abuse Act**

#### **18 U.S.C. § 1030**

35. Plaintiff repeats and fully incorporates every allegation above as if fully set forth in this Count on his own behalf and on behalf of the Class Members.

36. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), regulates fraud and related activity in connection with computers, making it unlawful to intentionally access a protected computer used for interstate commerce or communication, without authorization or by exceeding authorized access to it and obtaining information from it.

37. Plaintiff's computers and mobile digital devices are "protected computers" within the meaning of CFAA because both are a high speed data processing device performing logical, arithmetic, or storage functions that are used in or affecting interstate or foreign commerce or communication. 18 U.S.C. §§1030(e)(1) and 1030(e)(2)(B).

38. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing Plaintiff's computers and mobile digital devices by circumventing Plaintiff's preferred privacy settings without authorization and obtained information from Plaintiff's iPad® and iPhone®. Defendant exceeded authorized access and used that access to obtain or alter information in Plaintiff's computers and mobile digital devices that Defendant was not entitled to obtain or alter in violation of 18 U.S.C. § 1030 (e)(6).

39. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a code and causing a cookie to be downloaded that would permit Defendant to override Plaintiff's privacy settings and download third-party tracking cookies to Plaintiff's computers and mobile digital devices. By accessing, collecting, and transmitting Plaintiff's viewing habits, Defendant intentionally caused damage and loss.

40. Plaintiff has suffered damage by reason of these violations by the "impairment to the integrity or availability of data, a program, a system, or information" within the meaning of 18 U.S.C. § 1030(e)(8).

41. Plaintiff has suffered loss by reason of these violations including, without limitation: the violation of the right of privacy; disclosure of personal information, personal identifying information, and interception of browsing information, data, and habits that should otherwise have been maintained as private.

42. Defendant's violations have caused loss to 1 or more persons during a 1-year period aggregating at least \$5,000 in value. 18 U.S.C. § 1030(c)(4)(A)(I).

43. Defendant's violations have caused damage affecting 10 or more protected computer during the course of a 1-year period. 18 U.S.C. § 1030(c)(4)(A)(VI).

44. Defendant's acts and omissions were knowing and/or reckless and are the proximate cause of harm and damage to Plaintiff.

45. Plaintiff's damages for these losses include, but are not limited to: the "reasonable cost[s]...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. Defendant's unlawful access to Plaintiff's computers, mobile digital devices, and electronic communications caused her irreparable injury. Unless restrained or enjoined, Defendant's Privacy Efforts are meaningless and Defendant will continue to engage in these types of acts. Plaintiff's remedy at law is inadequate to compensate him for these inflicted and threatened injuries, entitling Plaintiff to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

## **COUNT II**

### **Violations of Electronic Communications Privacy Act**

#### **18 U.S.C. §§ 2510-2522**

47. Plaintiff repeats and fully incorporates every allegation above as if fully set forth in this Count on his own behalf and on behalf of the Class Members.

48. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 ("ECPA"), regulates wire and electronic communications interception and interception of oral communications, making it unlawful to "willfully intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

49. The ECPA 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. 18 U.S.C. § 2520(a).

50. Plaintiff is a person whose electronic communication has been intercepted and intentionally used in violation of the ECPA. 18 § 2510(6).

51. The contents of data transmission from and to Plaintiff's iPad® and iPhone® constitute "electronic communications," of signs, signals, writing, images, sounds, *data*, or *intelligence of any nature* within the meaning of the ECPA. 18 § 2510(12).

52. Defendant's violated the ECPA by intentionally intercepting, endeavoring to intercept, by device or otherwise, Plaintiff's electronic communications, without Plaintiff's knowledge, consent, or authorization. 18 U.S.C. § 2511(1)(a).

53. Defendant's violated the ECPA by intentionally disclosing, or endeavoring to disclose, to other persons the contents of Plaintiff's electronic communication without Plaintiff's knowledge. Defendant knew or had reason to know that the information was obtained through the interception of Plaintiff's electronic communication in violation of 18 U.S.C. § 2511(1)(c).

54. Defendant's violated the ECPA by intentionally using, or endeavoring to use, the contents of Plaintiff's electronic communication without Plaintiff's knowledge. Defendant knew or had reason to know that the information was obtained through the interception of Plaintiff's electronic communication in violation of 18 U.S.C. § 2511(1)(d).

55. Defendant's intentional interception of these electronic communications for an unlawful purpose, was made with Defendant's knowledge or having reason to know, that the electronic communications were obtained through interception.

56. Defendants are directly and/or vicariously liable for these violations. Plaintiff seeks statutory damages as provided under 18 U.S.C. § 2520(c) of whichever is the greater of \$100 a day for each day of violation or \$10,000 as well as injunctive and other equitable or declaratory relief as may be appropriate. Statutory damages consistent with subsection (c) will be proven at trial.

57. Plaintiff also seeks an award of reasonable attorney's fees and reasonably incurred litigation costs.

### **COUNT III**

#### **Violations of Florida Deceptive and Unfair Trade Practices Act**

#### **Fla. Stat. §§ 501.201-501.213**

58. Plaintiff repeats and fully incorporates every allegation above as if fully set forth in this Count on his own behalf and on behalf of the Class Members.

59. The Florida Legislature enacted the Florida Deceptive and Unfair Trade Practices Act ("FDUPTA) in 1972 to provide strong legal protection to consumers "from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202.

60. Patterned after the Federal Trade Commission Act, FDUPTA differs in part from its federal counterpart in that it provides a private right of action FDUPTA creates a private cause of action for declaratory and injunctive relief for "anyone aggrieved by a violation of this part." Fla. Stat. § 501.211(1).<sup>9</sup> FDUPTA also permits an aggrieved party to recover of actual damages, plus attorney's fees and court costs. Fla. Stat. § 501.211(1).

---

<sup>9</sup> FDUPTA defines "violation of this part" to mean "any violation of this act or the rules adopted under this act and may be based upon any of the following as of July 1, 2006: (a) Any rules



61. Plaintiff is a consumer as defined by FDUPTA. Fla. Stat. § 501.203(7).

62. Defendant is engaged in trade or commerce under FDUPTA because Defendant advertises, solicits, provides offers, or distributes its Google™ search engine service and other products and services ubiquitously in Florida. Fla. Stat. § 501.203(8).

63. By intentionally circumventing privacy restrictions on Plaintiff's computers and mobile digital devices without his consent and by failing to disclose this activity to Plaintiff, Defendant willfully engaged in unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade and commerce. Fla. Stat. § 501.204(1).

64. Defendant knows its privacy terms and conditions and overall Privacy Effort to be false, deceptive, and untrue. Had Plaintiff known that Defendant's products and services would track and record online activity in the manner intended by Defendant, Plaintiff would not have consented to online tracking.

65. As a direct and proximate result of Defendant's acts and violations of FDUPTA, Plaintiff has suffered actual injury and damages.

66. Plaintiff seeks a declaratory judgment and court order enjoining the Defendant from engaging in the above-described wrongful acts in the future. Plaintiff additionally seeks relief in the form of restitution and disgorgement.

---

promulgated pursuant to the Federal Trade Commission Act, 15 U.S.C. ss. 41 et seq.; (b) The standards of unfairness and deception set forth and interpreted by the Federal Trade Commission or the federal courts; (c) Any law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices." Fla. Stat. § 501.203(3).

67. Additionally Plaintiff makes claims for all available damages as well as for attorney's fees and costs as provided in Fla. Stat. § 501.625.

#### **COUNT IV**

##### **Violations of Florida Communications Fraud Act**

##### **Fla. Stat. § 817.034**

68. Plaintiff repeats and fully incorporates every allegation above as if fully set forth in this Count on his own behalf and on behalf of the Class Members.

69. At all times relevant to this action, Plaintiff had legal title to the iPad<sup>®</sup> and iPhone<sup>®</sup> referenced above, and a license to use the integrated Safari<sup>®</sup> web browser for its intended purpose, which are referenced throughout this Complaint.

70. If you are a Safari<sup>®</sup> web browser user, the default privacy settings of your browser tells Safari<sup>®</sup> to accept cookies only from the sites that you visit. The setting prevents outside sources from leaving cookies on your machine that you did not agree to accept. For example, if you visit your favorite news site to read a story and you load an iFrame<sup>10</sup> with contents from another site, Safari<sup>®</sup> will not save the cookie from the other site.

71. Defendant knowingly developed a code, comprised of just over two dozen lines, to override this privacy setting Safari<sup>®</sup> web browser. While the user is browsing the web, this code uses a blank form, submitted silently in the background as the page loads and without the user's knowledge or consent to "trick" Safari<sup>®</sup> into accepting cookies from unauthorized sources.

72. While it is unclear how long defendant engaged in this activity, the exploit became known in some code developer circles in 2010. The ability for developers, programmers,

---

<sup>10</sup> Inline Frames, or iFrames, are windows cut into the webpage you are viewing that allows you to view another page on that site or another page away from the site without reloading the entire page.

and companies to take advantage of the work around did not become known to the ordinary, average person like Plaintiff.

73. Defendant took advantage of Plaintiff's lack of awareness: it developed the code and engaged in a practice of monitoring and tracking Internet presence, usage, movements, history, preferences, and locations, without Plaintiff's knowledge and consent.

74. Defendant engaged in a systematic, ongoing course of conduct that it actively concealed from Plaintiff. Defendant used the trappings of communications technology and the appearance of privacy to induce Plaintiff to visit its websites while concealing its identity and activities in the background. In so doing, Defendant deceptively overcome Plaintiff's normal resistance to sales pressure by delivering a personalized, third party sales message to him, in violation of § 817.034 of the Florida Statutes.

75. Defendant has engaged in and has furthered a systematic, ongoing course of conduct with the intent to defraud and/or the intent to obtain property by false or fraudulent pretenses, representations, or promises, or willful misrepresentations of future acts.

76. Defendant's conduct resulted in the temporary or permanent deprivation of Plaintiff's right to use his computers and mobile digital devices and their respective integrated Safari® web browser as he intended. Additionally, Defendant deprived Plaintiff of the benefit of privacy. In so doing, Defendant impermissibly violated Plaintiff's rights and interests by: dispossessing him of its use; wrongfully obtaining information from it that he would not otherwise have voluntarily shared; gleaned a profile from his online activity to deliver personalized sales content to him; and appropriating both the property and information for its own use and for the use of third parties that were not entitled to it.

77. Plaintiff is entitled to recover any and all damages it sustained as a result of such trespass, in an amount to be determined at trial.

## COUNT V

### **Trespass to Property (Chattels)**

78. Plaintiff repeats and fully incorporates every allegation above as if fully set forth in this Count on his own behalf and on behalf of the Class Members.

79. At all times relevant to this action, Plaintiff had legal title to the iPad<sup>®</sup> and iPhone<sup>®</sup> referenced above, and a license to use the integrated Safari<sup>®</sup> web browser for its intended purpose, which are referenced throughout this Complaint.

80. Plaintiff's computers and mobile digital devices and their respective integrated Safari<sup>®</sup> web browser, data, and privacy interests are each considered "property" having "value" within the meaning of Fla. Stat. §§ 817.034(3)(c) and (e).

81. Defendant's intentional development and use of code to override Plaintiff's Safari<sup>®</sup> web browser privacy settings is the "use of communication technology," "use of a communication," and are a deliberate effort to "communicate" in order to "obtain" the "right to property or a benefit" and "to appropriate [] property to one's own use or to the use of any other person not entitled [to it]" within the meaning of Fla. Stat. § 817.034.

82. The pattern of criminal "communications" under Fla. Stat. § 817.034(3)(a), included, but are not limited to: the electronic transmission of Defendant's code over the Internet, the transmission and placement of a cookie on Plaintiff's computers and mobile digital devices; the interference with their intended functionality; and Defendant's amassing, acquiring, and using information derived from these acts to benefit from advertising and analytics services it sells to advertisers. Defendant's intentional acts are a pattern of illegal activity in violation of

Fla. Stat. § 817.034 and demonstrate criminal intent to receive proceeds derived, directly or indirectly, from a pattern of criminal activity within the meaning of Fla. Stat. § 772.103(1).

83. Defendant intentionally, and without justification, intermeddled and interfered with Plaintiff's computers and mobile digital devices by interfering with their respective Safari® web browser's built-in privacy settings, constituting a trespass to personal property. Defendant impaired the condition, quality, and value of Plaintiff's computers and mobile digital devices, which affirmatively blocked third-party cookies that would prevent Defendant and third parties to obtain information from his computers and mobile digital devices while he browsed the internet. Plaintiff did not configure his computers and mobile digital devices to share information in this way.

84. Defendant's unwanted intrusion deprived Plaintiff of his full use, enjoyment, and possession of his computers and mobile digital devices and impeded his personal choice and preferences concerning the manner in which he shared specific information on the Internet with third-parties.

85. Defendant's intentional trespass and interference proximately caused damage to Mr. Heretck, including, but not limited to, damage to the functionality of his computers and mobile digital devices and their respective integrated Safari® web browser, caused damage to Plaintiff's rights to dominion and control over his property, and damage to the confidential nature of the information he sought to protect. As a result, Defendant's caused Plaintiff's property and privacy interest to greatly diminish in value and deprived him of the intended use of these computers and mobile digital devices. Defendant's trespass interfered with, and damaged, the integrity and functionality of Plaintiff's computers and mobile digital devices and data.

86. Defendant will continue to commit these types of acts and, therefore, Defendant's trespass threatens to cause irreparable harm to Plaintiff and the Class Members, for which their remedy at law is not adequate to compensate them for the injuries inflicted and threatened.

87. Defendant's acts, omissions and violations of Fla. Stat. §§ 772.103(1) and 817.043 are the direct and proximate cause of damage and injury to Plaintiff.

88. By reasons of Defendant's violations of Fla. Stat. §§ 772.103(1) and 817.043, Plaintiff has a civil cause of action against Defendant and is entitled to threefold the actual damages he sustained in an amount to be proven at trial, but, at a minimum he is entitled to minimum damages in the amount of \$200 along with reasonable attorney's fees and court costs in the trial and appellate courts, which is consistent with the Florida Civil Remedies for Criminal Practices Act, Fla. Stat. §§ 772.101 – 772.19 and § 817.034(3)(e).

## COUNT VI

### **Unjust Enrichment/Restitution**

89. Plaintiff repeats and fully incorporates every allegation above as if fully set forth in this Count on his own behalf and on behalf of the Class Members.

90. Defendant's active concealment of its intent to use Plaintiff's web enabled devices to track Internet presence, usage, movements, history, preferences, and locations, without Plaintiffs' knowledge or consent induced Plaintiff to prolonged, continued use of the Google™ search engine and related with insufficient privacy protections in place.

91. Plaintiff conferred a benefit on Defendant by prolonged and continued unprotected use of the Google™ search engine and related sites under circumstances in which it would be unjust to permit Defendant to retain the benefits conferred.

92. Specifically, Defendant has unlawfully compiled information about Plaintiff's Internet presence, usage, movements, history, preferences, and locations without his informed consent. Defendant has profited from the collection of this information, amassed a virtual profile of Plaintiff's online behavior, and has stored this information indefinitely on its servers.

93. Defendant unjustly received benefits at Plaintiff's expense through its wrongful conduct, including Defendant's unfair business practices as well as Defendant's trespass. Defendant continues to unjustly retain these benefits at Plaintiff's and the Class Members' expense. It would be unjust for Defendant to retain any value obtained as a result of this wrongful conduct.

94. Plaintiff does not have an adequate remedy at law to compensate him for these inflicted and threatened injuries, entitling Plaintiff to remedies including declaratory and injunctive relief. Plaintiff also seeks restitution and disgorgement of profits that Defendant Derived from the sale of this information.

### **RELIEF SOUGHT**

**FOR ALL THESE REASONS**, Plaintiff, Kenneth W. Heretick, individually and on behalf of all others similarly situated, seeks relief as more fully set forth in this Complaint as follows:

95. For an order certifying that the action may be maintained as a class action, under Rule 23, Federal Rules of Civil Procedure and certifying Plaintiff, Kenneth W. Heretick, as Class Representative, and designating his counsel as counsel for the class;

96. For an award of equitable relief as follows:

a. Enjoining Defendant from engaging in similar unfair, unlawful, deceptive, and fraudulent misconduct in the future;

b. Requiring defendant to purge and securely destroy all data and analytics concerning the Class Members that Defendant garnered from tracking information obtained in unlawful ways;

c. Requiring Defendant to make full restitution of all monies wrongfully obtained as a result of the wrongful conduct described in this Complaint;

d. Requiring Defendant to disgorge all ill-gotten gains flowing from the wrongful conduct described in this Complaint;

e. Requiring Defendant to engage in a correct notice campaign;

f. Requiring Defendant's to immediately cease its wrongful conduct, including, but not limited to Defendant's self-serving attempts to "remove" tracking cookies on Plaintiff's and Class Members' computers and mobile digital devices;

97. For an award of attorney's fees and costs;

98. For an award of statutory damages under the applicable statutes to be determined at trial;

99. For an award of damages to be determined at trial; and

100. For any further legal and equitable relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on issues so triable.

Respectfully submitted,

BY:

John Yanchunis, Esquire



FBN: 0324681  
[iyanchunis@forthepeople.com](mailto:iyanchunis@forthepeople.com)  
MORGAN & MORGAN, P.A.  
201 North Franklin Street, 7th Floor  
Tampa, Florida 33602  
(813) 223-5505 Telephone  
(813) 223-5402 Facsimile  
Counsel for Plaintiffs