REGINALD TERRELL, ESQ.
THE TERRELL LAW GROUP
Post Office Box 13315, PMB #148
Oakland, California 94661
Telephone: (510) 237-9700
Facsimile: (510) 237-4616
Email: Reggiet2@aol.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ZETHA NOBLES, individually and on behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE, INC., a Delaware Corporation and POINTROLL, INC., a Delaware Corporation

Defendants.

CASE NO.: C12-03589

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Zetha Nobles ("Plaintiff"), by and through her attorney brings this action on behalf of herself and all others similarly situated against Google, Inc. and PointRoll, Inc. Plaintiff's allegations as to herself and her own actions, as set forth herein, are based upon her information and belief and personal knowledge, and all other allegations are based upon information and belief pursuant to the investigations of counsel. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (d) as set forth below.

I. NATURE OF THE ACTION

1. Plaintiff brings this consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), on behalf of herself and a proposed class of

similarly situated Individuals, (hereinafter referred to as the "Class Members"), who were victims of unfair, deceptive, and unlawful business practices; wherein their privacy, financial interests, and security rights were violated by Defendant Google, Inc. (hereinafter referred to individually as "Google"), and Defendant PointRoll, Inc. (hereinafter referred to individually as "PointRoll" and collectively with Google as "Defendants"), that acted individually, and in concert, to gain unauthorized access, use, and retention of Plaintiff's and Class members' data contained within their computing devices, which includes computers and mobile electronic devices used for communication, internet, and multimedia capabilities (hereinafter referred to collectively as "Computing Devices").

2. This Class Action lawsuit is brought by Plaintiff and Class Members who had their Computing Devices accessed without notice or consent, by circumventing their privacy settings in order to obtain personally identifiable information, including that of minor children, including, but not limited to, settling tracking mechanisms within their computing devices for subsequent online tracking by Defendants.

3. Defendants acted individually, and jointly, and knowing authorized, directed, ratified, approved, acquiesced in, or participated in conduct made the basis of this Class Action. Defendants used Plaintiff's and Class Members' Computing Devices to access, retain, and disclose personal information ("PI"), personally identifiable information ("PII"), and/or sensitive identifiable information ("SII") derived from Plaintiff's and Class Members' Computing Devices while they browsed online or wirelessly. Defendants accomplished this covertly, without actual notice, awareness, or consent and choice, and which information Defendants obtained deceptively, for purposes which included Defendants' commercial gain and nefarious purposes.

4. Defendants acted individually, and jointly, with entities involved in whole, or part, with advertising networks, data exchanges, traffic measurement service providers, and marketing and analytic service providers that develop and service websites (hereinafter referred to collectively as "Google Affiliates").

5. Each Google Affiliate committed acts made the basis of this action, individually and jointly, both intentionally and negligently, in whole or part, acting as a direct or contributory party to the action made the basis of this action. Pending discovery of the Google Affiliates' knowledge and involvement at the various stages of the acts complained of, and made the bases of this complaint, Plaintiff will amend the complaint to include such parties.

6. Defendants individually, and in concert with Google Affiliates, have been systematically engaged in and facilitated a covert operation of surveillance of Class Members and the following violations:

1) Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

2) Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*;

3) Violations of California Computer Crime Law, Penal Code § 502;

4) Violations of California's Invasion Of Privacy Act, California Penal Code § 630 *et seq.*;

5) Violations of California Unfair Competition Law, Business and Professions Code § 17200 *et seq.*;

6) Violations of California Consumers Legal Remedies Act, Civil Code § 1750 *et seq.*;

7) Violations of California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*;

8) Conversion;

9) Trespass to Personal Property / Chattels; and

10) Unjust Enrichment.

II. JURISDICTION AND VENUE

7. This Court has diversity jurisdiction in this case under a Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). This complaint states claims on behalf of a national class of consumers who are minimally diverse from Defendants. The amount in controversy exceeds $5 million, exclusive of interest and costs. The class consists of more than one hundred members.

8. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 as this action arises in part under a federal statute, the Computer Fraud and Abuse Act.

9. This Court has supplemental jurisdiction with respect to the pendent state law claims under 28 U.S.C. § 1367.

10. This Court has personal jurisdiction over Defendants because some of the acts alleged herein were committed in the state of California and because Defendants are registered to do business in this state and systematically and continuously conduct business here.

11. Venue is proper in this Court under 28 U.S.C. § 1391 because Google is a corporation headquartered in this District and/or because Defendants' improper conduct occurred in, was directed from, and/or emanated from this District.

12. **INTRADISTRICT ASSIGNMENT**: Pursuant to Civil Local Rule 3-2(e), this case shall be assigned to the San Jose Division as it arises from Santa Clara County where

Defendant Google is headquartered and where the actions alleged as the basis of this claim took place.

III. PARTIES

13. Plaintiff is an individual who owns and uses Apple's Safari and Microsoft's Internet Explorer ("IE") browsers that were protected by default privacy settings and/or higher privacy settings to restrict the ability of websites that use persistent browser cookies in collecting users' PI, PII, and SII.

14. Plaintiff Zetha Nobles is a resident of Oakland, Alameda County, California.

15. On information and belief, Plaintiff Zetha Nobles incorporates all allegations within this complaint.

16. At all relevant times herein, Villegas owned Computing Devices, including a personal computer with IE and a mobile device which had Apple's Safari browser, and used the Computing Devices, and on one or more occasions during the class period, in the city of residence and accessed the following websites reportedly associated with Defendants:

a. http://allrecipes.com/

b. http://www.businessweek.com/

c. http://www.cbsnews.com/

d. http://www.foodnetwork.com/

e. http://www.huffingtonpost.com/

f. http://www.meriam-webster.com/

g. http://www.washingtonpost.com/

17. Defendants, acting in concert individually and jointly, gained unauthorized access to, and unauthorized use of Nobles' Computing Device data.

18. Defendant Google, Inc. is a publicly traded Delaware corporation headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043 (Santa Clara County, California). Google does business throughout the United States.

19. Google is the owner and operator of the website located at http://www.Google.com, as well as a provider of advertising services through doubleclick.net.

20. Defendant PointRoll, Inc. is a publicly traded Delaware corporation headquartered at 7950 Jones Branch Drive, McLean, Virginia 22102. PointRoll does business throughout the United States.

21. PointRoll, a rich media advertising company, entered into a contract with Defendant Google, a California Corporation, and the acts made the basis of this action emanated to and from the Defendant Google's servers located in Mountain View, California.

22. PointRoll is the owner and operator of the website located at http://www.Pointroll.com, and provides digital marketing solutions and technology for rich media campaigns in interactive advertising,

23. On February 17, 2012, Jonathan Mayer, a Stanford researcher, published a study, "Web Policy – Do Not Track, Measurement, Privacy," ("Mayer Study") which "found that a PointRoll cookie helper script circumvents Safari's cookie blocking." In a blog post, PointRoll said it "conducted a limited test within the Safari browser to determine the effectiveness of our mobile ads," but claims it does not currently use the technique mentioned in Mayer's report.

IV. GENERAL ALLEGATIONS

I. A Brief Overview

24. On October 13, 2011, Defendant Google signed a consent order with the FTC which barred it from making misrepresentations regarding its privacy policies, required the

implementation of a comprehensive privacy program, and the retention of an independent third-party professional to access its privacy controls.

25. On October 19, 2011, the World Wide Web Consortium ("W3C"), the main international standards organization for the World Wide Web, announced that Google was one of its sponsors for the W3C Organization Sponsor Program, a program to enhance the W3C's capacity to support the deployment of web standards:

> "W3C has been a cornerstone component of the World Wide Web's evolution and Google is pleased to be able to support and participate in its process," said Vint Cerf, Chief Internet Evangelist at Google and an Internet pioneer.

W3C, "W3C Welcomes Google as First Gold Sponsor, Adobe Backs Initiative Supporting W3C Mission at Silver Level," (last accessed February 21, 2012), available online at: http://www.w3.org/2011/09/sponsor-pr.html.

26. During this week of October 13-19, 2011, while Defendant Google was agreeing to new privacy constraints and accepting accolades, it was also circumventing the privacy settings on Computing Devices for billions of Internet users, intentionally ignoring a cornerstone component of the World Wide Web's evolution: Platform for Privacy Preferences ("P3P").

27. On February 17, 2012, a research study by Jonathan Mayer, revealed Defendants Google and PointRoll were circumventing and exploiting the Safari browser in order to place diagnostic tools to track Safari browser users' activity. A research study by Microsoft confirmed the same exploits for users of Internet Explorer.

28. While the Mayer Study can be credited with revealing the Defendants' recent activities, a past study by Professor Lorrie Faith Cranor of Carnegie Mellon University first revealed these practices by some entities in September 2010 in a study titled "Token Attempt:

The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens."

29. Google's Senior Vice President of Communications Policy, Rachel Whetstone, issued a statement, noting in part in response to its practice, "that it is impractical to comply with Microsoft's request while providing modern web functionality." GreekWire.com, Todd Bishop, "Google: Microsoft's IE gotcha based on outdated, little-used privacy protocol," (last accessed February 21, 2012), available online: http://www.geekwire.com/2012/google-microsofts-gotcha-based-outdated-littleused-privacy-protocol.

30. Interestingly enough, the privacy setting protections not afforded Internet users involved with Defendants, claimed by Google to be archaic and impractical, are at the same time sought by Defendant Google: it uses a valid P3P syntax for its advertising sites.

31. An analysis using "Fiddler 2," a Web Debugging Proxy which logs all HTTP(S) traffic between your computer and the Internet, (last accessed on: February 22, 2012) online: http://fiddler2.com/fiddler2/, revealed the following: P3P Header is present: policy ref= http://www.googleadservices.com/pagead/p3p.xml, CP= "NOI DEV PSA PSD IVA PVD OTP OTR IND OTC" compact policy token is present. Date: Wednesday, 22 February, 2012 11:41:22 GMT.

32. P3P provides protection like a fortress around one's Computing Devices. Defendants' actions have unleashed a "Trojan Horse" of entities armed with every conceivable tracking tool into Plaintiff's and Class Members' Computing Devices. Due to the amount of third-parties associated with Defendants, the task to identify and delete all tracking tools implemented will be a Herculean task. As such, analysis of each "cookie" that now exists in each

of Plaintiff's and Class Members' Computing Devices is needed, requiring a "toxic cookie cleanup."

33. Plaintiff and Class Members do require the use of *authorized* cookies; thus they cannot merely push one button and delete all tracking devices. As such, since the identifying of entities associated with each cookie residing within the Plaintiff's and Class Members' Computing Devices are unknown, but at least some include Defendants' cookies, an analysis of each cookie is required and appropriate detection required. An estimate of such a requirement is in excess of ten thousand dollars ($10,000) per Plaintiff and Class Member.

II. Background: Web Browser's Incorporation of P3P for Cookie Filtering

34. P3P, the Platform for Privacy Preferences, provides a language and process that websites can use to post their privacy policies in a machine-readable form – that is, a form that can be processed by software such as web browsers. A website can post a full P3P policy, describing a variety of its privacy practices, or a "Compact Policy," describing its uses of browser cookies.

35. In 2001, Microsoft released version 6 of its market-leading Internet browser software, Internet Explorer ("IE6"), and included in it the capabilities to process websites' P3P Compact Policies. IE6 processed websites' Compact Policies automatically and, based on privacy settings that Microsoft set by default and that users could adjust, automatically allowed or restricted websites' storage of cookies on users' computers.

36. Before P3P, a privacy-conscious Internet user who wanted to learn about websites' cookie practices had only one choice – to read the privacy policy of every website visited – and to do so often, given that many websites advised users to "check back regularly to view updates to this policy."

37. This approach to managing cookies raised problems for users:

a. It is effectively impossible for a user to take the time to read the privacy policy of every website visited – and to do so continually to stay abreast of changes.

b. It is challenging for a user to try to interpret websites' privacy policies because, even among websites with substantially similar privacy practices, each website describes its practices in different ways and with varying levels of detail.

c. It is difficult for a user to determine which details of a website's privacy policy apply to which parts of the website, since a website's privacy practices may vary from page to page, such as a home page where the user signs up to use the website, a shopping-cart page where the user's purchase selections are listed, or a checkout page where the user provides credit card and shipping information.

d. It is impossible for a user to read a website's privacy policy "manually" without actually visiting the website, which means the user has to visit a website and receive whatever cookies the website delivers before the user has the chance to learn what the site's practices are.

38. The advent of P3P helped address these issues, as follows:

a. P3P provided a common language and syntax that websites could use to provide machine-readable versions of their privacy policies, including cookie-specific Compact Policies. *See* "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Group Note, Nov. 2006, available at http://www.w3.org/TR/P3P11 (last accessed on February 21, 2012).

b. P3P privacy statements could be quickly read by the user's web browser each time the user directed the browser to access a web page.

c. P3P permitted websites to offer granular privacy policies, tailored to the unique cookie practices of specific web pages within a website.

d. P3P-enabled web browsers could alert users to a websites' privacy practices before the user actually communicated with, and received cookies from, the website, and could automatically filter and restrict cookies based on the users' privacy settings, including default privacy settings.

39. In a world in which websites automatically and non-transparently examine a user's every online movement, IE6 gave users the ability to have their computers automatically examine the abbreviated privacy information that websites choose to disclose in their Compact Policies. Subsequent versions of IE gave users the same or better capabilities. IE assessed websites' cookie policies for users before the users even visited and acquired cookies from websites. In addition, in response to the users' privacy settings, IE could take certain actions in response to the P3P information it acquired, such as accept, reject, or restrict the cookies that websites transmitted to users.

40. Compact Policies, such as those that IE enabled users to assess automatically through their web browser, are expressed as a series of codes, called "tokens," each of which represents a standardized privacy expression defined in the P3P specification. For example, in the following Compact Policy:

CP= "NOI DSP COR NID ADMa OPTa OUR NOR"

The "NID" token means that no identified user information is collected by the web pages to which the Compact Policy applies or, if it is collected, it is anonymized in a way that cannot reasonably be reversed to reveal the user's identity; and the "OUR" token means that identified

user information is shared only with an agent whose use of the information is restricted to the purposes stated by the website. Likewise, the other tokens have predetermined meanings.

41. Under IE's default privacy settings, a website's unsatisfactory P3P Compact Policy can lead to several consequences. IE allows or limits cookies in different ways, depending on the statements in the Compact Policy and whether the web entity offering the policy is a first party (a website that the user explicitly chooses to visit) or a third party (such as entities that display advertisements on a first-party website). For example, if a first-party website's Compact Policy states that the website shares user PII without user consent, IE downgrades the website's "persistent" cookie to a "session" cookie – i.e., one that expires at the end of the user's browser session.

42. Persistent cookies serve as an important device for websites to identify users and collect their information; the release of IE6 prompted many websites to implement P3P Compact Policies so they could continue to set persistent cookies on the computers of users who adopted IE6.

III. Defendants' Misuse of P3P

43. On February 17, 2012, Jonathan Mayer, a Stanford researcher published a study, "Web Policy- Do Not Track, Measurement, Privacy" that revealed the Defendants were intentionally circumventing Safari privacy features. Microsoft researchers also completed a study that showed similar circumvention.

A. The Mayer Study

> Apple's Safari web browser is configured to block third-party cookies by default. We identified four advertising companies that unexpectedly place trackable cookies in Safari. Google and Vibrant Media intentionally circumvent Safari's privacy feature.

> Media Innovation Group and PointRoll serve scripts that appear to be derived from circumvention example code....
>
> 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 their current domain....
>
> These allowances in the Safari cookie blocking policy enable three potentially undesirable behaviors by advertising networks, analytics services, social widgets, and other 'third-party websites.' If a company operates both a first-party website and a third-party website from the same domain, visitors to the first-party website will be open to cookie-based tracking by the third-party service....
>
> Separating first-party websites from third-party services improves security: interactions between google.com content and other websites could introduce vulnerabilities. The domain separation also benefits user privacy: Google associates user account information with google.com cookies. By serving its third-party services from other domains, Google ensures it will not receive google.com cookies, and therefore will not be able to trivially identify user activities on other websites.

"Web Policy" (last accessed on: February 21, 2012), available online at:

http://webpolicy.org/2012/02/17/safari-trackers/.

B. Microsoft Study

> When the IE team heard the Google had bypassed user privacy settings on Safari, we asked ourselves a simple question: is Google circumventing the privacy preferences of Internet Explorer users too? We've discovered the answer is yes: Google is employing similar methods to get around the default privacy protections in IE and track IE users with cookies....
>
> We've found that Google bypasses the P3P Privacy Protection feature in IE. The result is similar to the recent reports of Google's circumvention of privacy protections in Apple's Safari Web

> browser, even though the actual bypass mechanism Google uses is different....
>
> Google secretly developed a way to circumvent default privacy settings established by a... competitor, Apple... [and] Google then used the workaround to drop ad-tracking cookies on the Safari users, which is exactly the sort of practice that Apple was trying to prevent. Third-party cookies are a common mechanism used to track what people do online. Safari protects its users from being tracked this way by a default user setting that blocks third-party cookies....
>
> By default, IE blocks third-party cookies *unless* the site presents a P3P Compact Policy Statement indicating how the site will use the cookie and that the site's use does not include tracking the user. Google's P3P policy causes Internet Explorer to accept Google's cookies even though the policy does not state Google's intent.
>
> P3P, an official recommendation of the W3C Web standards body, is a Web technology that all browsers and sites can support. Sites use P3P to describe how they intend to use cookies and user information. By supporting P3P, browsers can block or allow cookies to honor user privacy preferences with respect to the site's stated intentions....
>
> Technically, Google utilizes a nuance in the P3P specification that has the effect of bypassing user preferences about cookies. The P3P specification (in attempt to leave room for future advances in privacy policies) states that browsers should ignore any undefined policies they encounter. Google sends a P3P policy that fails to inform the browser about Google's use of cookies and user information. Google's P3P policy is actually a statement that it is not a P3P policy. It's intended for humans to read even though P3P policies are designed for browsers to "read."

"Google Bypassing User Privacy Settings" (last accessed on February 21, 2012) online at:

http://blogs.msdn.com/b/ie/archive/2012/02/20/google-bypassing-user-privacy-settings.aspx

44. Defendant Google did not refute the findings, and although individuals had set their privacy settings to their preferences, knowingly circumvented users' preferences:

> "Microsoft uses a 'self-declaration' protocol (known as 'P3P') dating from 2002 under which Microsoft asks websites to represent their privacy practices in machine-readable form. It is well known – including by Microsoft – that it is impractical to comply with Microsoft's request while providing modern web functionality. We have been open about our approach, as have many other websites." Google's Senior Vice President of Communications and Policy, Rachel Whetstone.

IV. Harm

A. "Toxic Cookies" Require a "Toxic Cookie Cleanup"

45. Defendants have left tracking mechanisms and files within Plaintiff's and Class Members' Computing Devices. Like a toxic oil spill in the Gulf of Mexico causing loss and/or damage to the area residents, embedded "toxic cookies" now require a "toxic cookie cleanup."

46. Plaintiff and Class Members demand that Defendants return their Computing Devices to the state that existed prior to any and all activity implemented by Defendants and Google Affiliates. Such a demand is premised on the fact that although Defendants have ceased setting the cookies, Defendants may still continue their tracking practices using such tracking mechanisms. Plaintiff's and Class Members' Computing Devices are at risk, and Plaintiff and Class Members do not desire to accept such a risk.

47. Defendants' actions have caused harm to the Plaintiff and Class Members, including, but not limited to, the following:

a. Loss due to costs associated with requiring Computing Device forensics to investigate, locate, and delete any and all tracking mechanisms located within Plaintiff's and Class Members' Computing Devices without removing authorized cache storage cookies;

b. Impairment of the Computing Devices;

c. Loss due to "interception of internet service";

d. Use of bandwidth to set Defendants' tracking mechanisms;

e. Use of bandwidth for ad "calls" and ad insertion; and

f. Loss due to the collection, storage, use, and sale of the Plaintiff's and Class Members' personal information.

48. Plaintiff and Class members use their Computing Devices' cache to store and use data, including, but not limited to, files of interest, website passwords, and bookmarks. Plaintiff and Class Members do not want to use the Computing Devices' software to delete their entire cache but only that data within their hardware associated with Defendants and Google Affiliates. This task, though, requires accessing the Plaintiff's and Class Members' hard drive to examine each and every data file.

49. Cleaning software provides the cache deletion mechanisms that delete the browser cache. This purges all ETag values. The cost for cleaning is quite low if a user merely runs the cache deletion of all browsers; however, Plaintiff and Class Members do not desire to delete all cache cookies.

50. Plaintiff's and Class Members' concerns relate to data remanence, or the residual representation of data that remains even after attempts have been made to remove or erase the data. This residue may result from data being left intact by a nominal file deletion operation, by reformatting the storage media that does not remove data previously written to the media, or through physical properties of the storage medium that allow previously written data to be recovered.

51. It is a misconception about deleting computer files that by simply pressing the delete button, emptying the "Recycle Bin," or even formatting the drive that it deletes all files.

Information still remains on the hard disk drive ("HDD"). Formatting the HDD also does not erase hidden files. The data is not permanently erased and formatting still leaves unused parts of the HDD and the swap file holding data.

52. When information is written to a drive, the location of the information is stored in a file that resembles a table of contents for a book. On computers running DOS and Windows operating systems, the File Allocation Table ("FAT") or the Master File Table ("MFT") holds this information. When a file is deleted, the FAT or MFT is updated to tell the computer the space on the HDD is available; however, the actual data is not deleted until it is overwritten with new data. This is the reason why computer forensic software is able to recover data. Using software undelete tools, files that were accidentally or otherwise deleted can be restored.

53. The U.S. Department of Defense 5220.22-M standard for disk-sanitization is the most rigorous data wipe procedure. This wiping standard requires seven passes, with each pass formed of three different data wipes. The HDD is rewritten and covered with random patterns. With each wipe, the deleted data becomes harder to piece back together.

54. The most effective and efficient way to clean a computer would be to indiscriminately erase ALL tracking files on the computer which would include cookies, flash cookies, HTML5 storage, etc. To go through and erase solely the Defendants' related files would take extra time and would bear the risk of not eliminating all of the potential threats. Plaintiff and Class Members desire to have their Computing Devices restored to the state the hardware existed in before Defendants' activities without deleting any of their cache data.

B. <u>Loss and/or Damage in Excess of $5,000.00 ("CFAA")</u>

55. Plaintiff and Class Members have suffered loss and/or damages that exceed five thousand dollars ($5,000.00) in order to mitigate Defendants' invasive actions by expending

time, money, and resources, to investigate and repair their Computing Devices, a conduct violation as defined in the Computer Fraud and Abuse Act ("CFAA"), Title 18, United States Code, Section 1030. The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Under the CFAA, "loss" is treated differently from "damage," and is defined as "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). Accordingly, Plaintiff must claim economic loss or damages in an amount aggregating at least $5,000 in value during any 1-year period to one or more individuals. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I).

56. Plaintiff's and Class Members' economic loss involves costs to obtain a complete forensic examination of their Computing Devices. Estimates for such services exceed thirty-five (35) hours at a cost of three hundred and fifty dollars ($350.00) per hour, or exceeding a total cost of twelve thousand two hundred and fifty dollars ($12,250.00) per device:

> "A complete examination of a single 80 GB hard drive can have over 18,000,000 pages of electronic information and may take between 15 to 35 hours or more to examine, depending on the size and types of media. A reasonable quote can be obtained prior to the investigation's start. This time could increase or decrease, depending upon the type [of] operating system used, the type of data contained within, and the size and amount of data in question. Computer forensic investigations have an unusually high return on investment. The total computer forensic price can average from $250 to $350 an hour."

New York Computer Forensics Services, "Computer Forensics Frequently Asked Questions" (last accessed February 21, 2012), available online at:

http://www.newyorkcomputerforensics.com/learn/forensics_faw.php

57. The average costs of Computing Devices range from one hundred and fifty dollars ($150.00) to fifteen hundred dollars ($1,500.00). Plaintiff and Class Members use such devices to conduct both personal and commercial business. Any interference of any kind to such devices would interfere with their personal enjoyment and/or commercial use. Plaintiff and Class Members were harmed due to any delay in use once the Defendants' actions became known, and delay in time to investigate and repair any loss and/or damage. Moreover, Plaintiff's and Class Members' loss shall include the purchase of a new Computing Device's hardware and operating system.

58. Plaintiff and Class Members purchased Computing Devices with consideration of costs, speed, and security features. The cost of the hardware and software necessary for the security features were factored into the total price of the Computing Devices; thus a specific sum was allocated to the cost of including the security features. As such, Defendants' circumvention of Plaintiff's and Class Members' Computing Devices rendered such hardware and software protections purchased within the Computing Devices worthless.

59. Native Security Software was provided to Plaintiff and Class Members within their Computing Devices when purchased for use on a trial basis, with generally an average sixty (60) day trial period. Common Native Security Software is a Norton or McAfee product. Once the trial period expired, the Plaintiff and Class Members downloaded software or purchased such at an electronics retailer. Security Software costs average approximately seventy five dollars ($75.00) to one hundred and fifty dollars ($150.00) per Computing Device to provide continued security protection. Such Security Software purchased was rendered worthless due to Defendants' activities made the basis of this action.

60. Defendants' harm to Plaintiff and Class Members involves a loss that includes the purchase of an HDD, transferring of files, and re-installation of an operating system. Hidden files on an HDD actually store data long after deleted and can be recovered by experts. As an alternative to clearing all cache and cookies, a user would need to purchase a brand new HDD, reinstall Windows, and have their authorized data from the hard drive transferred to a new HDD. A retail price for this would average one hundred dollars ($100.00) for the HDD and approximately $150-$250 for the operation of transferring the files, installing Windows, etc., or about $300-$350 total at a market price.

61. Defendants' harm to Plaintiff and Class Members involves paying a computer technician to spend hours and hours reading every single cookie file, cache file, etc., though this is not very efficient. Regardless, a technician could spend approximately ten (10) to twenty (20) hours going through each and every cookie file. If a Computing Device has 18,000,000 cookies, it would take substantial time on a Computing Device that has a lot of cookies to view each one individually. A technician shall have to indiscriminately read every line of every file of cache and analyze it, and delete Defendants' tracking files.

62. Plaintiff and Class Members that have their HDD/cache removed, but want to still use the infected hard drive must extract all the authorized data, and that would require additional costs for that process. Data transfer could be as much as $250. Plaintiff and Class Members must purchase a brand new HDD and all of their data (music, documents, etc.) must be transferred to the new HDD. Plaintiff's and Class Members' loss includes a cost of about $350 for the HDD and the service. However, programs cannot be transferred. For example, if Microsoft Office is installed on the old HDD, it has to be manually re-installed on the new HDD. This applies to all applications. Typically, that is the user's responsibility. Most computer technicians will not re-

install all of the programs for the user. It would be plausible to say that re-installing an average user's applications would take another three to four hours and thus cost an extra $400. Market cost to buy a new HDD and have all of a user's program and files transferred to it, so that they were made whole and in the same shape that they were in before, would cost approximately $750.

63. The issue is not that the cost is higher to delete the hidden files than the cost of a total replacement, i.e. buying a brand new computer; it's that a person's data is invaluable to them. Individuals have years' worth of research, bookmarks, and cache on their hard drive; thus user data is invaluable if lost.

C. Unauthorized Use of Bandwidth ("Bandwidth Hogs")

64. Defendants' activities of circumventing Plaintiff's and Class Members' Computing Devices and using such to conduct tracking required bandwidth. The problem is that the bandwidth used to complete Defendants' objectives had not been purchased by Defendants, but rather by the Plaintiff and Class Members.

65. Defendants caused an economic harm to the Plaintiff and Class Members that is actual, non-speculative, sum certain, tangible, and scientifically documented, and that was incurred by the unauthorized use of their Computing Devices' bandwidth; in that:

a. Plaintiff and Class Members purchased a monthly limited bandwidth data plan for their Computing Device from their provider.

b. Plaintiff and Class Members then accessed websites, "expecting" and agreeing to limited bandwidth consumption required and necessary to interact with the websites.

c. However, Defendants then redirected Plaintiff's and Class Members' Computing Devices to access their tracking mechanism and had HTTP cookies set after they have been deleted, and such was not "expected" by the user, not required to interact with the website, not agreed upon by the user, and not necessary to operate the Computing Devices.

d. Defendants then made "calls" directing Plaintiff's and Class Members' Computing Devices to third parties for marketing purposes, thereby depleting the purchased and linked bandwidth data plans of the Plaintiff and Class Members, and such was not "expected" by the user, not required to interact with the website, not agreed upon by the user, and not necessary to operate the Computing Devices.

66. Bandwidth is the amount of data that can be transmitted across a channel in a set amount of time. Any transmission of information on the internet includes bandwidth. Similar to utility companies, such as power or water, the "pipeline" is a substantial capital expenditure, and bandwidth usage controls the pricing model. Hosting providers charge users for bandwidth because their upstream provider charges them and so forth until it reaches the "back bone providers." Retail providers purchase it from wholesalers to sell to its consumers.

67. Bandwidth to the Computing Device is like gasoline to a motor vehicle. Without it, the device is inoperable. Defendants require bandwidth to conduct their tracking activities made the basis of this action. However, the bandwidth used is that of the Plaintiff and Class Members. Like an individual that fills up their car's gas tank to find it empty because their neighbor drove their car without permission, Plaintiff and Class Members pay monthly

bandwidth use fees for their own use and not by Defendants to conduct their tracking business. From the Defendants' perspective, reducing their own bandwidth usages reduces their own costs.

68. Defendants' unauthorized interception and use of Plaintiff's and Class Members' electronic communications, include, but are not limited to, the following:

a. Interception of the Plaintiff's and Class Members' electronic communications after Plaintiff and Class Members visited the websites and then used their Computing Devices to limit access for tracking; including, but not limited to, deleting cookies and implementing mechanisms to limit re-spawning made the basis of this action;

b. Use of the Plaintiff's and Class Members' bandwidth by Defendants to install their tracking mechanisms within their Computing Devices;

c. Use of the Plaintiff's and Class Members' bandwidth by Defendants to activate, use, and monitor their online activities;

d. Use of the Plaintiff's and Class Members' bandwidth by Defendants to add tracking mechanisms;

e. Use of the Plaintiff's and Class Members' bandwidth by Defendants to provide access to, and use by Google affiliates of their Computing Devices;

f. Use of the Plaintiff's and Class Members' bandwidth by Defendants to conduct advertising procedures, including, but not limited to, "calls" to third party web analytic vendors, advertising networks, and their affiliates.

69. The technology behind the World Wide Web is the Hypertext Transfer Protocol (HTTP) and it does not make any distinction as to the types of links; thus, all links are functionally equal. Resources may be located on any server at any location. When a website is visited, the browser first downloads the textual content in the form of an HTML document. The downloaded HTML document may call for other HTML files, images, scripts and/or style sheet files to be processed. These files may contain tags which supply the URLs that allow images to display on the page. The HTML code generally does not specify a server, meaning that the web browser should use the same server as the parent code. It also permits absolute URLs that refer to images hosted on other servers. Once the application has stored the data, it will attempt to send information back to affiliated servers. In most cases this is done every time a user opens and closes a browser. The data is continually tracked. A website that enables tracking does not take just one sample; it will record every use of the website for the life of that website on a user's computer and the user's information is sent automatically at a user's bandwidth expense.

70. Ads consume vast amounts of bandwidth, which results in slowing a user's internet connection by using their bandwidth and diminishing the Computing Devices' battery life in order to retrieve advertisements. Web analytics devour more bandwidth than ads by accessing bandwidth to download and run ad script; thus Plaintiff and Class Members that did not access ads on a website still had the Defendants use their bandwidth for its tracking:

> When you're probing, you're using a user's battery and data when they don't know about it, but it's a faster way to build up data cause you're not waiting for the user to check in a few times a day. You're pinging in 100 times a day....

Yarrow, Jay "Everything You Need to Know About How Phones are Stalking You Everywhere" (last accessed February 21, 2012) available online at: http://www.businessinsider.com/skyhook-ceo-2011-4#ixzz1PTSNQ1pq

71. Advertisers are now using the Internet as their primary ad-delivery pipe, continually uploading and downloading data from networks, causing substantial bandwidth use. Ads that were hidden in content or bundled used substantial bandwidth, as did updates. Web analytics activities delayed Plaintiff's and Class Members' movement on websites, and used their bandwidth to carry out Defendants' activities.

72. Web analytic vendor and ad networks use ad content, such as streaming video and audio, that requires excessive use of Plaintiff's and Class Members' bandwidth. This is due in part to the fact that there was no incentive to reduce the ad size used because they could directly pass costs for bandwidth and ad delivery content to Plaintiff and Class Members, without the Plaintiff and Class Members having any notice. For example, while Plaintiff and Class Members were browsing a website, at the same time web analytic vendors and ad networks were silently harvesting personal data and sending it to remote servers using Plaintiff's and Class Members' bandwidth.

73. Defendants' use of Plaintiff's and Class Members' bandwidth for their data mining activities is similar in nature to a practice called "hot linking," wherein one server uses another server's bandwidth to send data. While it slows down the server, it also allows bandwidth costs to be transferred to another server. Defendants' data mining activities produce similar unauthorized bandwidth use. While only tech savvy individuals are aware that their Computing Devices are used as a server without their knowledge or consent, fewer individuals are aware of the extent that web analytic vendors and ad networks make "calls" to third parties, and of the amount of user's bandwidth used when a user merely accesses a site.

74. Excluding the amount of bandwidth that the Plaintiff and Class Members use, the amount necessary to operate their computer, the amount expected by the user's interaction with

the website, and that of which was agreed upon by the user, Defendants' unauthorized data mining activities caused substantial bandwidth use to the Plaintiff and Class Members that resulted in actual out of pocket expenditures. Defendants' activities include, but are not limited to, the following:

a. Transmittal of and access to Plaintiff's and Class Members' accessed websites and tracking mechanisms set on their Computing Devices;

b. Loading of ads first before content, bundling ads, and ads with excessive bandwidth;

c. Use of Software Development Kits ("SDKs"), and their functions within Plaintiff's and Class Members' Computing Devices';

d. Harvesting of Plaintiff's and Class Members' Computing Devices' data;

e. Harvesting of Plaintiff's and Class Members' PI, PII, and SII;

f. "Background" activities including "data mining";

g. "Push notifications" of content to user's Computing Devices; and

h. Re-direction of Plaintiff's and Class Members' Computing Devices to make "calls" to Defendants and Google Affiliates for marketing purposes.

75. The amount of bandwidth use on Computing Devices can be measured directly by analyzing the logged traffic use, which varies generally between 0 bytes and about 500k bytes per session. The traffic use, whether expected by the user or not, is part of the normal operation of the Computing Device. Website traffic analysis shows the majority of the traffic is tracking code integration and the directing of traffic to third party servers. The traffic to third parties for

marketing purposes is not required nor authorized by the user; moreover, the user is never prompted to allow it or notified that it has occurred.

76. The basic nature of HTTP is a challenge-response protocol. For each request, there is necessarily a response. Conventional technical usage would refer to the challenge-response pair as a single "call".

77. In HTTP/1.0, an HTTP request requires a new TCP/IP connection to be initiated and then torn down after the response. This causes a significant amount of bandwidth to be wasted doing the "bookkeeping" for each TCP/IP session. The excessive bandwidth use is related to defining how to issue multiple requests and receive responses using a single TCP/IP connection. Websites must be able to open essentially only a limited amount of connections, whatever the designated "simultaneous network connections" setting is to the server for the entire session.

78. Although memory is technically any form of electronic storage, it is used most often to identify fast, temporary forms of storage. If a user's Computing Device's CPU had to constantly access the HDD to retrieve every piece of data it needs, it would operate very slowly.

79. The cache increases transfer performance. A part of the increase similarly comes from the possibility that multiple small transfers will combine into one large block. The main performance gain occurs because the same datum will be read from cache multiple times, or that written data will soon be read. A cache's sole purpose is to reduce accesses to the underlying slower storage.

80. CPUs need quick and easy access to large amounts of data in order to maximize their performance. If the CPU cannot get to the data it needs, it literally stops and waits for the data to be processed.

81. Defendants' services must interface with, and draw bandwidth from, Plaintiff's and Class Members' Computing Devices' limited bandwidth data plan in order to complete its tracking practices. Like a "bad" neighbor that sneaks over in the dead of night to plug in an extension cord into their neighbor's electrical outlet to "suck out" kilowatts, Defendants were "hogging" the Plaintiff's and Class Members' purchased and limited bandwidth plan, and not reimbursing Plaintiff and Class Members for using their limited data plan. The economic harm is actual, non-speculative, out of pocket, sum certain, and scientifically documented:

> "If consumers perceive that rich media ads and other marketing activities affecting their consumption of bandwidth, and that they are paying to watch ads, it could [ ] affect mobile advertising."

Chantal Tode, "T-Mobile's new pricing reflects concern over growing bandwidth use" (last accessed February 21, 2012) available online at:http://mobilemarketer.com/cms/news/carrier-networks/10014.html

V. CLASS ALLEGATIONS

82. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(a), and (b)(1), (b)(2) and/or (b)(3) on behalf of herself and the following class:

> All persons residing in the United States who possessed a Computing Device which had a Safari or IE browser that had Defendants circumvent their Computing Devices' privacy preferences ("Class").

83. The Class Period is defined as the time period applicable under the claims to be certified.

84. Excluded from the Class are Defendants, their assigns, and successors, legal representatives, and any entity in which Defendants have a controlling interest. Also excluded is the judge to whom this case is assigned and the judge's immediate family.

85. Plaintiff reserves the right to revise this definition of the Class based on facts learned as litigation progresses.

86. The Class consists of millions of individual and other entities, making joinder impractical.

87. The claims of Plaintiff are typical of the claims of all other members of the Class.

88. Plaintiff will fairly and adequately represent the interests of the Class. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions, including privacy cases. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Class and have the financial resources to do so. Neither Plaintiff nor her counsel any interests adverse to those of the Class.

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

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

91. The factual and legal bases of Defendants' liability to Plaintiff and to the other Class Members are the same, resulting in injury to Plaintiff and all of the other Class Members.

Plaintiff and the other Class Members have all suffered harm and damages as a result of the Defendants' wrongful conduct.

92. There are many questions of law and fact common to Plaintiff and the Class, and those questions predominate over any questions that may affect only individual Class Members. Common and predominant questions for the Class include, but are not limited to, the following:

a. What was the extent of Defendants' business practice of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data?

b. What information did Defendants collect from their business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data, and what did they do with that information?

c. Whether users, by virtue of visiting websites with Defendants' tracking mechanisms, had pre-consented to the operation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data;

d. Was there adequate notice, or any notice, of the operation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data provided to Plaintiff and Class Members?

e. Was there reasonable opportunity to decline the operation of Defendants' business practices of circumventing users' Computing Device security

settings to transmit, access, collect, monitor, and remotely store users' data provided to Plaintiff and Class Members?

f. Did Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data disclose, intercept, and transmit PI, PII or SII?

g. Whether Defendants' devised and deployed a scheme or artifice to defraud or conceal from Plaintiff and the Class Members Defendants' ability to, and practice of, circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data, for their own benefit, personal information, and tracking data from Plaintiff's and the Class members' personal Computing Devices via the ability to track their data on their Computing Device;

h. Whether Defendants engaged in the deceptive acts and practices in connection with their undisclosed and systemic practice of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data on Plaintiff's and the Class Members' personal Computing Devices and using that data to track and profile Plaintiff's and the Class Members' Internet activities and personal habits, proclivities.

i. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030?

j. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*

k. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the California's Computer Crime Law, Penal Code § 502?

l. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the California Invasion of Privacy Act, Penal Code § 630 *et seq.*?

m. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Consumers Legal Remedies Act, ("CLRA") California Civil Code § 1750 *et seq.*?

n. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Unfair Competition, California Business and Professions Code § 17200 *et seq.*?

o. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit,

access, collect, monitor, and remotely store users' data violate the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*?

p. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data involve a Conversion?

q. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data involve a Trespass to Personal Property / Chattels?

r. Did the implementation of Defendants' business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data result in Unjust Enrichment?

s. Are any of the Defendants liable under a theory of aiding and abetting one or more of the remaining Defendants for violations of the statutes listed herein?

t. Are the Defendants liable under a theory of civil conspiracy for violations of the statutes listed herein?

u. Are the Defendants liable under a theory of unjust enrichment for violations of the statutes listed herein?

v. Whether Defendants participated in and/or committed or are responsible for violation of law(s) complained of herein;

w. Are Class Members entitled to damages as a result of the implementation of Defendants' conduct, and, if so, what is the measure of those damages?

x. Whether Plaintiff and Class Members have sustained damages as a result of Defendants' conduct, and, if so, what is the appropriate measure of damages;

y. Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

z. Whether Plaintiff and Class Members are entitled to punitive damages, and, if so, in what amount?

93. The questions of law and fact common to the Class predominate over any questions affecting only individual members and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

94. Based on the foregoing allegations, Plaintiff's legal theories for relief include those set forth below.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
(Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

95. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein.

96. Plaintiff's and the Class Members' Computing Devices are computers used in and affecting interstate commerce and communication and are therefore "protected computers" as defined in the Computer Fraud and Abuse Act (the "CFAA"), 18 U.S.C. § 1030(e)(2).

97. Defendants violated the CFAA, 18 U.S.C. § 1030(a)(4) in that they knowingly and with intent to defraud, accessed the protected Computing Devices of Plaintiff and the Class

Members without authorization, or exceeding authorized access, and by means of such conduct, furthered the intended fraud and obtained things of value.

98. As described above, Defendants published an invalid P3P Compact Policy to transmit false information to Plaintiff's and Class Members' browsers and to thereby surreptitiously gain access to and place persistent cookies onto their Computing Devices.

99. Defendants acted without authorization or exceeding authorization in that Plaintiff and the Class Members did not give Defendants permission or consent to place persistent cookies on their Computing Devices. In fact, they reasonably believed that Safari and IE would block such cookies from being placed on their Computing Devices or downgrade such cookies to the status of session cookies.

100. Defendants' conduct was done knowingly and with intent to defraud in that Defendants created and used an invalid P3P Compact Policy for the purpose of circumventing the cookie-filtering functions of Plaintiff's and the Class Members' browsers and because they had no legitimate purpose for using an invalid P3P Compact Policy.

101. Through Defendants' conduct it was able to further their intended fraud of placing persistent cookies on Plaintiff's and Class Members' Computing Devices and using such cookies to collect and maintain Plaintiff's and Class Members' PI, PII and SII, and to share that information with third parties without the knowledge, consent, or authorization of Plaintiff and Class Members.

102. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered harms and losses that include those described above.

103. Defendants' unlawful access to Plaintiff's and Class Members' Computing Devices through the use of invalid P3P Compact Policies constituted a single act that resulted in an aggregated loss to Plaintiff and the Class Members of at least $5,000 within a one-year period.

104. Therefore, Plaintiff and the Class Members are entitled to compensatory damages.

105. In addition, Defendants' unlawful access to Plaintiff's and Class Members' Computing Devices has caused Plaintiff and Class Members irreparable injury.

106. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiff's and Class Members' remedy at law is not adequate to compensate them for these inflicted, imminent, threatened, and continuing injuries, entitling Plaintiff and the Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

SECOND CAUSE OF ACTION
(Violation of the Electronic Communications Privacy Act 18 U.S.C. § et seq.)

107. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein.

108. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of herself and the Class.

109. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 *et seq.*, ("ECPA"), regulates wire and electronic communications interception and interception of oral communications, and makes it unlawful for a person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

110. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiff's and Class Members' electronic communications, without knowledge, consent or authorization.

111. At all relevant times, Defendants engaged in business practices of intercepting the Plaintiff's and Class Members' electronic communications, which included endeavoring to intercept the transmission of a user's Computing Devices' activities and interactions between the user and its contact online from within their Computing Devices. Once the Defendants obtained the data, they used such to aggregate Computing Device data of the Plaintiff and Class Members as they used their Computing Devices.

112. The contents of data transmissions from and to Plaintiff's and Class Members' Computing Devices constitute "electronic communications" within the meaning of 18 U.S.C. § 2510.

113. Plaintiff and Class Members are "person[s] whose … electronic communication is intercepted … or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

114. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept Plaintiff's and Class Members' electronic communications.

115. Defendants violated 18 U.S.C. § 2511(a)(c) by intentionally disclosing, or endeavoring to disclose, to any other person the contents of Plaintiff's and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiff's and Class Members' electronic communications.

116. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiff's and Class Members' electronic communications.

117. Defendants' intentional interception of these electronic communications without Plaintiff's or Class Members' knowledge, consent, or authorization was undertaken without a facially valid court order or certification.

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

119. Defendants unlawfully accessed and used, and voluntarily disclosed, the contents of the intercepted communications to enhance their profitability and revenue through advertising. This disclosure was not necessary for the operation of Defendants' system or to protect Defendants' rights or property.

120. ECPA, 18 U.S.C. § 2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the ECPA.

121. Defendants are liable directly and/or vicariously for this cause of action. Plaintiff and Class Members therefore seek remedy as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and reasonable attorneys' fees and other litigation costs reasonably incurred.

122. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

123. Plaintiff and the Class Members, pursuant to 18 U.S.C. § 2520, are entitled to 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 Defendants' profits obtained from the above-described violations. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's remedy at law is not adequate to compensate for these inflicted and threatened injuries, entitling Plaintiff to remedies including injunctive relief as provided by 18 U.S.C. 2510.

THIRD CAUSE OF ACTION
(Violations of Cal. Penal Code 502
The California Computer Crime Law ("CCCL"))

124. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein.

125. Defendants violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking, and using Plaintiff's and the Class Members' Computing Devices.

126. Defendants accessed, copied, used, made use of, interfered with, and/or altered, data belonging to Plaintiff and Class Members: (1) in and from the state of California; (2) in the home states of the Plaintiff and the Class Members; and (3) in the states in which the servers that provided services and communication links between Plaintiff and Class Members and the websites with which they interacted were located.

127. Cal. Penal Code § 502(j) states: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to

have personally accessed the computer, computer system, or computer network in each jurisdiction."

128. Defendants have violated California Penal Code § 502(c)(1) by knowingly and without permission altering, accessing, and making use of Plaintiff's and Class Members' Computing Devices and using the data in order to execute a scheme to defraud consumers.

129. Defendants have violated California Penal Code § 502 (c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiff's and Class Members' Computing Devices, computer system and/or computer network.

130. Defendants have violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiff's and Class Members' computer system, and/or computer network.

131. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" means "any set of computer instructions that are designed to … record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information."

132. Defendant have violated California Penal Code § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiff and the Class Members and websites; specifically, web page interactions that propagate a harvesting software placed there by Defendants.

133. As a direct and proximate result of Defendants' unlawful conduct within the meaning of California Penal Code § 502, Defendants have caused loss to Plaintiff and the Class Members in an amount to be proven at trial. Plaintiff and the Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).