ORIGINAL

David Parisi (SBN 162248)
dcparisi@parisihavens.com
Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
Parisi & Havens LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299

Joseph H. Malley (not admitted)
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

Counsel for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

BRIAN WHITE; R.H., a minor, by and through her parent, JEFF HALL; A. A., a minor, by and through her parent, JOSE AGUIRRE; J. H., a minor, by and through his parent, JEFF HALL; KIRA MILES; TONI MILES; and TERRIE J. MOORE, individuals, on behalf of themselves and others similarly situated,

Plaintiffs,

v.

CLEARSPRING TECHNOLOGIES, INC., a Delaware Corporation; WALT DISNEY INTERNET GROUP, a California unincorporated association; DEMAND MEDIA, INC., a Delaware Corporation; PROJECT PLAYLIST, INC., a Delaware Corporation; SOAPNET, LLC, a Delaware

CASE NO. CV10 5948

JURY DEMAND

CLASS ACTION COMPLAINT FOR:

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

2. Violation of California's Computer Crime Law, Penal Code § 502;

3. Violation of California's Invasion Of Privacy Act, California Penal Code § 630;

Corporation; SODAHEAD, INC., a Delaware Corporation; USTREAM, INC., a Delaware Corporation; WARNER BROS. RECORDS, INC., a Delaware Corporation;

Defendants.

4. Violation of California's Consumer Legal Remedies Act, Civil Code § 1750;
5. Violation of California's Unfair Competition Law, Business and Professions Code § 17200;
6. Trespass to Personal Property / Chattels
7. Unjust Enrichment

Plaintiffs, Brian White, R. H., a minor, by and through her parent, Jeff Hall, A. A., a minor, by and through her parent, Jose Aguirre, J. H., a minor, by and through his parent Jeff Hall, Kira Miles, Toni Miles, and Terrie J. Moore, on behalf of themselves and all others similarly situated, by and through their attorneys, Parisi & Havens LLP, and Law Office of Joseph H. Malley, P.C., as and for their complaint, and demanding trial by jury, allege as follows upon information and belief, based upon, *inter alia*, investigation conducted by and through their attorneys, which are alleged upon knowledge, sue Defendants Walt Disney Internet Group, Clearspring Technologies, Inc., Demand Media, Inc., Project Playlist, Inc., Inc., Soapnet, LLC, SodaHead, Inc., Ustream, Inc., and Warner Bros. Records, Inc. Plaintiffs' allegations as to themselves and their own actions, as set forth herein are based upon their personal knowledge, and all other allegations are based upon information and belief pursuant to the investigations of counsel. Based upon such investigation, Plaintiffs believe that substantial evidentiary support exists for the allegations herein or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and discovery.

NATURE OF THE ACTION

1. Plaintiffs bring this consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3on behalf of themselves and a class of similarly situated Internet users, each a "Class Member" of the putative "Class," as further described herein, who were victims of fraud and unfair business practices; wherein their privacy, financial interests, and computer security rights, were violated by the following defendants ("Defendants"): Clearspring Technologies, Inc., (hereinafter referred o as "Clearspring"), and websites affiliated individually with Clearspring, referred collectively to as, "Clearspring Flash Cookie Affiliates," and individually as: Walt Disney Internet Group (hereinafter referred to as "Walt Disney Internet Group"), Demand Media, Inc. (hereinafter referred to as "Demand Media"), Project Playlist, Inc., (hereinafter referred to as "Project Playlist"), Soapnet, LLC (hereinafter referred to as "Soapnet"), SodaHead, Inc. (hereinafter referred to as "SodaHead"), Ustream, Inc. (hereinafter referred to as "Ustream"), and Warner Bros. Records, Inc. (hereinafter referred to as "Warner Bros. Records") by setting Flash cookies on their users' computers to use the Flash Media Player local storage Flash on those computers to back up browser cookies for the purposes of restoring them later.

2. Clearspring Flash Cookie Affiliates each independently, with Clearspring, knowingly authorized, directed, ratified, approved, acquiesed in, or participated in conduct made the basis of this Class action, which included, but was not limited to, setting of an online tracking device which would allow access to and disclosure of Internet users' online activities as well as personal information ("PI"), personal identifying information ("PII"), and/or sensitive indentifying information ("SII") derived from such online activities, including users' activities on non-Clearspring Flash Cookie Affiliates' websites, and which Defendants accomplished covertly, without actual notice to users, awareness by users, or consent and choice of users, and which information Defendants obtained deceptively, for purposes not disclosed within their Terms of Service and/or

Privacy Policy, which purposes included Defendants' commercial gain and nefarious purposes.

3. Plaintiffs and Class Members are consumers in the United States who use their computers to access websites on the Internet and who configured their web browser privacy settings to deny permission for third parties to set cookies on their computers, and visited online one of the Clearspring Flash Cookie Affiliate's websites.

4. Defendants Clearspring Flash Cookie Affiliates acted with Defendant Clearspring, independently of one another, and hacked the computers of millions of consumers' computers to plant rogue, cookie-like tracking code on users' computers. With this tracking code, Defendants circumvented users' browser controls for managing web privacy and security.

5. Plaintiffs and Class Members that visited the websites of the Clearspring Flash Cookie Affiliates had tracking codes installed on their computers by Defendant Clearspring acting in concert with the respective Clearspring Flash Cookie Affiliates, without notice or consent, and which tracking codes could not easily be detected, managed or deleted. In cooperation with the Clearspring Flash Cookie Affiliates, Clearspring planted its own tracking code on users' computers—but not in a browser cookie. Clearspring and Clearspring Flash Cookie Affiliates stored tracking code as Adobe Flash Media Player local shared objects (LSOs). Adobe Flash Media Player is software that enables users to view video content on their computers.

6. Once the tracking code was installed by the Defendants, such provided the mechanism to track Plaintiffs and Class Members that visited non-Clearspring Flash Cookie Affiliates websites by having their online transmissions intercepted, without notice or consent; moreover if the user deleted the browser cookie, the Flash cookie would be used to "re-spawn" the browser cookie.

7. Defendants perpetrated this exploit so they could obtain personal

identifying information, monitor users, and to sell users' data. The personal information Defendants misappropriated and compiled, with information provided from Clearspring and Clearspring Flash Cookie Affiliates includes details about user profiles to identify individual users and track them on an ongoing basis, across numerous websites, even spotting and tracking users when they accessed the web from different computers, at home and at work. This sensitive information may include such things as users' video viewing choices and personal characteristics such as gender, age, race, number of children, education level, geographic location, and household income, what the web user looked at and what he/she bought, the materials he/she read, details about his/her financial situation, his/her sexual preference, his/her name, home address, e-mail address and telephone number, and even more specific information like health conditions, such as DEPRESSION.

8. For example, shown below are the computer logs of an individual, name redacted for privacy purposes, suffering from DEPRESSION, that visited a health-related website on March 1, 2010 at 3:13:57 AM to watch a video related to DEPRESSION. The computer activity log notes the users' name and the individual's computer id, represented by an eight (8) digit hexadecimal ID code composed of numbers and letters from the users' hard drive are as follows:

URL : http://depression.[name redacted].com/pub_videoplayer/player/ut.swf
Filename : [name redacted]-ut.sol
Created Time : 3/1/2010 3:13:57 AM
Modified Time : 3/1/2010 3:13:57 AM
File Size : 67
File Path : C:\Users\[name redacted]\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\[user id redacted]\depression.[name redacted].com\pub_videoplayer\player\ut.swf\[name redacted]-ut.sol

URL : http://bin.clearspring.com
Filename : clearspring.sol
Created Time : 3/1/2010 3:22:26 AM
Modified Time : 3/4/2010 11:11:46 PM
File Size : 724
File Path : C:\Users\[name redacted]\AppData\Roaming\Macromedia\Flash

Player\#SharedObjects\[user id redacted]\bin.clearspring.com\clearspring.sol

9. Defendants' perpetration of this exploit was independently confirmed in a report issued by academic researchers and titled, "Flash Cookies and Privacy," which found that:

a) A user visiting site would receive a standard, browser cookie, and an identical "Flash cookie."
b) If the user deleted the browser cookie, the Flash cookie would be used to "re-spawn" the browser cookie.
c) These operations happened without any notice to the user and without any consent from the user.

"Flash Cookies and Privacy," A. Soltani, S. Canty, Q. Mayo, L. Thomas, C.J. Hoofnagle, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 (last accessed July 28, 2010).

10. Defendants' use of the Adobe Flash Media Player for tracking online users was condemned by Adobe:

> Adobe condemns the practice of using Local Storage to back up browser cookies for the purpose of restoring them later without user knowledge and express consent.

http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf (last accessed August 5, 2010)

11. Defendant Clearspring CEO admitted that Clearspring used tracking Flash cookies.

> Flash cookies were a mistake. The company says it no longer uses Flash cookies for tracking.
>
> CEO Hooman Radfar says Clearspring provides software and services to websites at no charge. In exchange, Clearspring collects data on consumers. It plans eventually to sell the data it collects to advertisers.

Angwin, Julia. "The Web's New Gold Mine: Your Secrets" *The Wall Street Journal*. July 30, 2010, http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748703940904575395

5073512989404.html (last accessed August 5, 2010)

JURISDICTION AND VENUE

12. Venue is proper in this District under 28 U.S.C. §1391(b) and (c) against all Clearspring Flash Cookie Affiliates. A substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District and Defendants conduct business with consumers in this District. Defendant Walt Disney Internet Group's principle executive offices and headquarters are located in this District at 500 S. Buena Vista St., Burbank, CA 91521. Defendant Demand Media's principle executive offices and headquarters are located in this District at 1333 Second Street, Santa Monica, CA 90401. Defendant Soapnet, LLC's principle executive offices and headquarters are located in this District at 3800 W Alameda Avenue, Burbank, CA 91505. Defendant SoadHead, Inc.'s principle executive offices and headquarters are located in this District at 15821 Ventura Blvd., Suite 260, Encino, CA 91436.

13. Subject-matter jurisdiction exists in this Court related to this action pursuant to 28 U.S.C. § 1332. The aggregate claims of Plaintiffs and the proposed Class Members exceed the sum or value of $5,000,000.00.

14. Venue is proper in this district and vests jurisdiction in the California state and federal courts in the district of the location of their principal corporate place of businesses. Thus, mandatory jurisdiction in this U.S. District Court vests for any Class Member, wherever they reside, for the online activity made the basis of this action which occurred within the United States. The application of the law of the State of California should be applied to any online activity made the basis of this action anywhere, within the United States, as if any and all activity occurred entirely in California and to California resident. Thus, citizens and residents of all states are, for all purposes related to this instant Complaint, similarly situated with respect to their rights and claims as California residents, and therefore are

appropriately included as members of the Class, regardless of their residency, or wherever the online activity occurred made the basis of this action.

15. Minimal diversity of citizenship exists in this action, providing jurisdiction as proper in the Court, since Defendants Demand Media, Walt Disney Internet Group, Soapnet and SodaHead are corporations headquartered in this District, and Plaintiffs include citizens and residents of this District, and assert claims on behalf of a proposed Class whose members are scattered throughout the fifty states and the U.S. territories; thus there is minimal diversity of citizenship between proposed Class Members and the Defendant.

16. The U.S. Central District of California is the judicial district wherein the basis of the conduct complained of herein involving the Defendants was devised, developed, implemented. The actual interaction of information and data was activated from, and transmitted to and from this District; therefore all evidence of conduct as alleged in this complaint is located in this judicial district.

PARTIES

17. Plaintiff A. A. ("A. A."), is a citizen and resident of Milwaukee, Wisconsin, (Milwaukee County), and a minor, represented by and through her parent, Jose Aguirre. On information and belief A. A. incorporates all allegations within this complaint. A. A. is a representative of the "U.S. Resident Class," defined within the Class Allegations. At all relevant times herein, A. A. was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) Warner Bros. Records

18. Plaintiff Jose Aguirre ("J. Aguirre"), is a citizen and resident of Milwaukee, Wisconsin, (Milwaukee County). On information and belief, J. Aguirre incorporates all allegations within this complaint. At all relevant times

herein, J. Aguirre was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) SodaHead

19. Plaintiff J. H. ("J. H."), is a citizen and resident of Forney, Texas, (Kaufman County), and a minor, represented by and through his parent, Jeff Hall. On information and belief, J. H. incorporates all allegations within this complaint. At all relevant times herein, J. H. was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) Project Playlist, Inc.

20. Plaintiff R. H. ("R. H."), is a citizen and resident of Forney, Texas, (Kaufman County), and a minor, represented by and through her parent, Jeff Hall. On information and belief, R. H. incorporates all allegations within this complaint. At all relevant times herein, R. H. was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) SodaHead

21. Plaintiff Kira Miles ("K. Miles"), is a citizen and resident of Lubbock, Texas, (Lubbock County). On information and belief, K. Miles incorporates all allegations within this complaint. At all relevant times herein, K. Miles was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) Demand Media

22. Plaintiff Toni Miles ("T. Miles"), is a citizen and resident of Odessa,

Texas, (Ector County). On information and belief, T. Miles incorporates all allegations within this complaint. At all relevant times herein, T. Miles was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) SodaHead

23. Plaintiff Terrie J. Moore ("Moore"), is a citizen and resident of Grain Valley, Missouri, (Jackson County). On information and belief, Moore incorporates all allegations within this complaint. At all relevant times herein, Moore was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) Soapnet

24. Plaintiff Brian White ("White"), is a citizen and resident of Diamond Bar, California, (Los Angeles County). On information and belief, White incorporates all allegations within this complaint. At all relevant times herein, White was an Internet user that, on one or more occasions during the Class period, in the city of residence, accessed online a website owned by the following named Clearspring Flash Cookie Affiliate:

a) Ustream

25. Defendant Clearspring Technologies, Inc. (hereinafter "Clearspring"), is a Delaware corporation which maintains its headquarters at 8000 Westpark Dr., Suite 625, McLean, Virginia 22102. Defendant Clearspring Technologies, Inc., does business throughout the United States, and in particular, does business in State of California and in this County.

26. Defendant Walt Disney Internet Group, (hereinafter "Walt Disney Internet Group"), is an unincorporated entity doing business in the State of

California. Walt Disney Internet Group maintains its headquarters at 500 S. Buena Vista St., Burbank, California 91521. Defendant Walt Disney Internet Group does business throughout the United States, and in particular, does business in State of California and in this judicial district.

27. Defendant Demand Media, Inc. (hereinafter "Demand Media"), is a Delaware corporation which maintains its headquarters at 1333 Second Street, Santa Monica, California 90401. Defendant Demand Media does business throughout the United States, and in particular, does business in State of California and in this judicial district.

28. Defendant Project Playlist, Inc. (hereinafter "Project Playlist"), is a Delaware corporation which maintains its headquarters at 444 High Street, Suite 300 Palo Alto, California 94301. Defendant Project Playlist does business throughout the United States, and in particular, does business in State of California and in this judicial district.

29. Defendant Soapnet, LLC (hereinafter "Soapnet"), is a Delaware company which maintains its headquarters at 3800 W Alameda Avenue, Burbank, California 91505. Defendant Soapnet does business throughout the United States, and in particular, does business in State of California and in this judicial district.

30. Defendant SodaHead, Inc. (hereinafter "SodaHead"), is a Delaware corporation which maintains its headquarters at 15821 Ventura Blvd., Suite 260, Encino, California 91436. Defendant SodaHead does business throughout the United States, and in particular, does business in State of California and in this judicial district.

31. Defendant Ustream, Inc. (hereinafter "Ustream"), is a Delaware corporation which maintains its headquarters at 274 Castro Street, Suite 204, Mountain View, California 94041. Defendant Ustream does business throughout the United States, and in particular, does business in State of California and in this judicial district.

32. Defendant Warner Bros. Records, Inc. (hereinafter "Warner Bros. Records"), is a Delaware corporation which maintains its headquarters at 75 Rockefeller Plaza, New York, New York 10019. Defendant Warner Bros. Records does business throughout the United States, and in particular, does business in State of California and in this judicial district.

33. This Class action does not include Clearspring affiliated corporations and websites which were not involved in whole, or part, setting, or allowing Clearspring to set, a flash cookie on its users' computer hard drive to use the local storage within the user's flash media player to back up browser cookies for the purpose of restoring them later without actual notice/awareness and consent/choice of the user.

34. This Class action does not include Clearspring affiliated corporations and websites which provided its users adequate actual notice and awareness, that personal information would be collected, and allowed users' choice as to how the personal information collected would be used, as it relates to information obtained by the placement of flash cookies on the users' computer hard drive and the use of user's local storage within their flash media player to back up browser cookies for the purpose of restoring them later without actual notice/awareness and consent/choice of the user.

35. This Class action does not include Clearspring affiliated corporations and websites which accessed the flash media player on a user's computer for its intended purpose, as governed by the flash media player's EULA, and was not related in whole, or part, on using the users' computer hard drive and using local storage within their flash media player to back up browser cookies for the purpose of restoring them later without actual notice/awareness and consent/choice of the user.

36. The conduct complained of includes, but not limited to, the interception of electronic communication of Plaintiffs and Class Members

involving non-Clearspring Flash Cookie Affiliates, obtained in transit and temporarily stored for a limited period in their computer's electronic storage. *In re: Doubleclick, Inc. Privacy Litigation,* 154 F. Supp.2d 497,00 Civ. 0641 (S.D.N.Y., March 28, 2001)

37. The conduct of Clearspring individually and in concert with the Clearspring Flash Cookie Affiliates, individually and jointly, is a fraud that has been perpetrated for years, facilitated, and coordinated, by some of the world's largest websites and the network advertising industry, thereby costing the Class upwards of tens of millions of dollars. Defendants have been systematically defrauding Class Members in a covert operation of surveillance made possible by their gross misconduct, negligence, apparent coordination, and actual fraud, and violating one (1) or more of the following:

a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"), against all Defendants;

b) California's Computer Crime Law, Penal Code § 502 (the "CCCL"), against All Defendants;

c) California's Invasion Of Privacy Act, California Penal Code § 630, against Clearspring;

d) California's Consumer Legal Remedies Act, Civil Code § 1750 ("CLRA");

e) California's Unfair Competition Law, Business and Professions Code § 17200 ("UCL");

f) Trespass to Personal Property / Chattels

g) Unjust Enrichment, against all Defendants.

38. The collection of data by Defendants was wholesale and all-encompassing. Data passing from the users' computers were acquired by Defendants without discrimination as to the kind, type, nature, or sensitivity of the data. Like the privacy one loses from an airport security body scanner, everything

passing through the consumer's Internet connection was intercepted by Defendants, claimed as their property, and traded as a commodity. Regardless of any representations to the contrary—all data—whether sensitive, financial, personal, private, complete with all identifying information, was intercepted, exposing users like "fish in a fishbowl."

STATEMENT OF FACTS

A. Background

39. This consumer class action involves a pattern of covert online surveillance, wherein the Clearspring Flash Cookie Affiliates, operated individually with Clearspring; associated in fact, targeted Internet users that visited Clearspring Flash Cookie Affiliates' websites, and knowingly, without the user's knowledge or consent; accessed the user's computer, transmitting a program, information, code, and command, to set a tracking device within the user's Flash media player, to intercept electronic communications, overriding user's security preferences, by setting a Flash cookie on the user's computer hard drive to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later, if deleted by its users. This practice also referred to as "browser cookie re-spawning," circumvented the user's intent to clear browser cookies. The objective of this scheme was the online harvesting of consumers personal information for online marketing activities. The Defendants' uniform business practice was as simple as it was deceptive and devious.

> We found that top 100 websites are using Flash cookies to "respawn," or recreate deleted HTTP cookies. This means that privacy-sensitive consumers who "toss" their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies. Few websites disclose their use of Flash in privacy policies…

Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, Chris Jay Hoofnagle, "Flash Cookies and Privacy" (10 August 2009), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

40. Defendants Clearspring Flash Cookie Affiliates' privacy documents omit entirely the actual identity of its association with Clearspring, limiting the user's awareness of, and an inability to determine accurately, the involvement of Clearspring, or locate the Clearspring website, compounded further by Clearspring defining its business as a media measurement and web analytics company while the Clearspring Flash Cookie Affiliates' privacy documents refer only to associations involving advertising networks.

41. Defendants Clearspring Flash Cookie Affiliates' privacy documents describe "associations," misleading the users which interpret such to be associated corporate subsidiaries, withholding accurate information that such includes other entities than advertising networks, such as: data exchanges, traffic measurement service providers, and marketing analytics service providers.

42. Defendant Clearspring Flash Cookie Affiliates' websites are owned by parent companies that have many subsidiaries and fail to provide adequate information about third-party information sharing, different than affiliate sharing, which is subject to more restrictions, including opt-in or opt-out consent requirements. These restrictions are based upon the heightened risk associated with sharing information with unrelated entities, which have different incentives than the entity that collected the user data.

43. Defendants Clearspring Flash Cookie Affiliates do not make adequate distinctions between sharing with affiliates, contractors, and third parties, instead, vaguely stating that they do not share user data with unrelated third parties and vaguely disclosing that they share data with affiliates. Users must interpret an affiliate to be a third party, but given the actual usage of these terms of Clearspring Flash Cookie Affiliates' privacy policies, that assumption would be mistaken.

44. Defendants Clearspring Flash Cookie Affiliate users are unable to identify the corporate families to which these Defendant websites belong; which

makes it difficult for a user to discover exactly who such associated entities are, thus their practices are deceptive. A practice is deceptive if it involves a representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment. The conflicting statements in the privacy policies would most likely confuse or mislead a reasonable consumer. The confusion would also likely be to their detriment, as surveys indicate that users do not want companies to collect data about them without permission.

45. Defendants Clearspring Flash Cookie Affiliates' privacy documents discuss that the data collection practices of entities associated with their corporations are outside the coverage of their privacy policies. This appears to be an attempt to create a critical loophole used by Defendant Clearspring Flash Cookie Affiliates compounding their attempts to violate the privacy protection of their users.

46. Defendants Clearspring Flash Cookie Affiliates' privacy documents fail to provide adequate notice that these Defendants allow access to personal behavioral data of their users, including but not limited to, such data embedded with their cookies, to Clearspring, which in turn shares the data with its marketing partners or corporate affiliates and subsidiaries, meaning that user behavior will be profiled by any other entities with whom those sites may choose to share this information. Defendants Clearspring Flash Cookie Affiliates state they do not share data with third parties, but they do share data with affiliates, suggesting that they only share data with companies under the same corporate ownership.

47. Defendant Clearspring's privacy documents referenced the use of Flash cookies, but state such is used only for audience measurement and not behavioral ad-targeting. The opt-out is inconspicuous on their privacy page and appears in a small font header in the corner of the page.

48. Defendant Clearspring's privacy documents do not expressly state that

if a Clearspring Flash Cookie Affiliate user opts out that behavioral information will not be collected and shared, but only that the Clearspring Flash Cookie Affiliate user will not receive Internet based advertising content from its "advertising delivery service"; moreover its opt-out "unique cookie value" includes identifying information which means the cookie is no longer non-unique.

49. Defendants' privacy documents falsely imply some level of protection for the user. Defendants' privacy documents are sufficiently vague so as to refrain from fully disclosing information to their users about what information is collected through their websites and their associated entities, how the information is used, and the purposes for the collection and use of this information, negating the possibility for their users to provide informed and meaningful consent to these practices. Without adequate notice and informed and meaningful user consent, users had no control over their personal information, thus, the potential privacy dangers were not readily apparent to most users.

50. Defendants' privacy documents require college-level reading skills for comprehension and include substantial legalese, ambiguous and obfuscated language designed to confuse, disenfranchise, and mislead the users.

51. Defendants' privacy documents incorporate a multitude of hedging and modality markers so as to minimize their use of covert surveillance technology and data-gathering tools, while sending mixed messages related to privacy controls, advising users that choosing to exercise such controls would cause in whole, or part, diminished functionality of their websites, while such documents emphasize all cookies are very small, thus unobtrusive, and pose no threat since "many websites use them."

52. Defendants' privacy documents fail to adhere to an adequate notice and choice regime, predicated on user choice, and informed by privacy policies. Defendants' privacy documents provided nuanced situations that created conditional yes or no answers to these basic questions about a site's data collection

and sharing practices, thus it is unclear how an average user could ever understand these practices since the nuances were not explained in the privacy policy. Choice, therefore, cannot be inferred.

53. Defendants' privacy documents fail to provide notice that their data storage practices as they relate to the period for which user data is stored, have no term period and are indefinite.

54. Defendants' privacy documents carefully attempt to parse the definitions of phrases related to their tracking activity. Their privacy documents are more nuanced than such categorized analysis allows for, omitting any direct reference to Flash cookies, embedding surveillance technology into the user's computer hardware, use of user's computer hardware to store data, use of technology to allow the perpetual online tracking and surveillance of any and all online Internet activity of the Clearspring Flash Cookie Affiliate user. They also refrain from disclosing that the Clearspring Flash Cookie Affiliate would use the user's local storage to back up browser cookies for the purpose of restoring them later without user knowledge and express consent, as evidenced by the attempt to hide its covert activity by referring to their use of "other technologies," or "similar technologies" to cookies and web beacons, in lieu of Flash cookies which would have perpetual existence on a user's computer and the ability to respawn, i.e. "zombie cookies."

55. Defendants' privacy documents' verbiage was deceptive by design. This deception is especially troubling when compared with the obligation imposed upon their online visitors to download, read, and comprehend the vast amount of documents required to protect one's online privacy, complicated by the cumulative effect of such task.

56. In addition to downloading, reading and comprehending all of the Walt Disney Internet Group privacy documents, its users would be required to locate the website for Clearspring and repeat this obligation for Clearspring's

privacy documents. To accentuate the improbability of completing this task though, Clearspring Flash Cookie Affiliate website visitors were not provided any information of the identity of Clearspring within Walt Disney Internet Group, nor any of the Clearspring Flash Cookie Affiliates', Terms of Service and Privacy Policy.

57. In addition to the Walt Disney Internet Group and Clearspring privacy documents, a user would be obligated to review their Flash media player's privacy documents. Some Internet users possess multiple Flash media players, and many are not aware of the identity of their Flash media player nor are provided information from Defendants as to the identity of the Flash media player being apprehended for use by the Clearspring Flash Cookie Affiliate and/or Clearspring. If a user could identify their involved Flash media player, and the identity of the corporate entity for the Flash media player, the user would have additional obligations imposed upon them to download, read, and comprehend the Flash media player's privacy documents, such as Adobe's, the largest Flash media player provider.

58. Clearspring Flash Cookie Affiliates' users' online privacy protection was premised upon imposed requirement to download, read and comprehend the accumulation of all privacy documents of Clearspring Flash Cookie Affiliate, Clearspring, and the user's Flash media player, such as Adobe.

59. A *millisecond* was the time allotted to an online visitor opening a Clearspring Flash Cookie Affiliates' webpage, before a Flash cookie was embedded within their computer and data collected immediately, without their awareness, knowledge or consent to such actions. Such occurred without the benefit of being provided adequate time to access, read, and attempt to comprehend the Terms of Service/Use and Privacy Policy for Clearspring Flash Cookie Affiliates' website, Clearspring's, and the website of the user's Flash media player. While only the most technical savvy online users were familiar with

cookies, a finite amount of individuals even knew about Flash cookies, let alone could possibly comprehend the technical aspects of Flash cookies inherent within the Defendants' privacy documents.

60. To put matters in perspective, a Herculean task would be required, and equate in work count to reading, in a *millisecond*, either the United States Constitution eleven (11) times, Plaintiffs' complaint twice, or one (1) of George Orwell's novels, or more appropriately,: Nineteen Eighty-Four:

> *"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."*

B. Traditional Online Advertising

61. Commercial websites, such as Clearspring Flash Cookie Affiliates, use online advertising in order to promote content to the consumers without charge and require online advertising to support this objective. Commercial websites, known as "publishers" allow portions of their web page to be sold to online advertising networks, which act as an intermediary between "publishers" and the "advertisers."

62. Most commercial websites that are advertising supported, allow the ad images to be served directly from the servers of the advertisers or an advertising network, and do not keep their advertisements locally. Rather, they subscribe to a media service that places those ads for them. This is accomplished by a media service.

63. Web advertisements provided by "third-party ad servers" inject their advertisements into hosting web pages. The web page upon which an

advertisement will appear reserves a blank space in the page's layout with a URL containing a third-party advertising server address. Whenever that page is displayed, the user's web browser will read the page, discover the URL address of the advertising server, and request a web page asset from it. This could be an image, Flash animation, video, or other resource from the third-party server. When the advertising asset is received by the browser, it will be inserted into the page to appear in the reserved location and become part of the delivered page.

64. Publishers desiring to identify and track users while they were on their site embed "first party" tracking devices, "session cookies," used to facilitate a user's activities within the selected website while actively on that site, and "persistent cookies," which exist beyond the period of the initial website session and provides tracking technology while a user visits all websites.

65. Online advertising companies use a tracking system to gauge webpages as activity while the user navigated online in and out of its advertising network, and "third-party cookies" accomplish this goal. In the process of advertising placement/injection, advertisers can place cookies on the user's machine. Since the advertisers place ads on multiple sites, the cookie allows the advertiser to observe the user's browsing behavior across many websites. Large ad-serving agents span significant portions of the World Wide Web and thereby acquire extensive behavioral data. The net result is that the user gets a cookie from the media service without ever having visited it.

66. Cookies typically are small files. The cookie text files themselves consist of strings of "name-value" pairs that reduce to code various pieces of information about an individual's computer, the browsing choices a person makes while accessing a Web site and any additional information a person discloses during a particular visit. While some cookies may contain minimal information, others may record a wide array of user-profiling information, IP numbers, shopping cart contents, user IDs, user-selected preferences, serial numbers,

frequencies of contact with companies, demographics, purchasing histories, credit-worthiness, social security numbers and other personal identifiers, credit card numbers, phone numbers, and addresses. In addition to that user specific information, the name-value pairs include basic parameters regarding the range of servers and sites that can access the cookie from an individual's hard drive as well as the cookie expiration date.

67. Cookies accumulate each time the property is set. Once the maximum pair limit is reached, subsequent set will push older name/value pair off in favor of the new name/value pair. As text, browser cookies are not executable. Because they are not executed, they cannot replicate themselves.

68. Cookies are based on a two-stage process. First the cookie is stored in the user's computer. The web server creates a specific cookie, which is essentially a string of text containing the user's preferences, and it transmits this cookie to the user's computer. The user's web browser receives the cookie and stores it on the computer. As a result, personal information is formatted by the web server, transmitted, and saved by the user's computer.

69. During the second stage, the cookie is non-transparently and automatically transferred from the user's machine to a web server. Whenever users direct their web browser to display a certain web page from the server, the browser will, without user knowledge, transmit the cookie containing personal information to the web server.

70. Cookies are normally only sent to the server setting them or a server in the same domain (*e.g.*, a cookie set by mail.abc.com could be shared with calendar.abc.com). These are called first-party cookies because they are set by the site displayed in the address bar of the Web browser. Third-party cookies, on the other hand, are typically used by advertising networks to track users across multiple websites where the networks have placed advertising—which allows the advertising network to target subsequent advertisements to the user's presumed

interests and also to limit the number of times a user is shown a particular ad.

71. Normal Internet cookies are limited in their size to four kilobytes. This was part of the RFC 2109 limitations standard which is conformed to by both Internet Explorer and Netscape and was compiled by The Internet Engineering Task Force (IETF). Cookies may hold text or array data, yet are still limited to a size of 4kb each. Normally cookies begin their existence in the memory of the browser and only if a cookie is given a longer life span than the life of the browser will it then be written to disk. Cookie specifications suggest that browsers should be able to save and send back a minimal number of cookies. In particular, an Internet browser is expected to be able to store at least 300 cookies of four kilobytes each, and at least 20 cookies per server or domain. The cookie setter can specify a deletion date, in which case the cookie will be removed on that date. If the cookie setter does not specify a date, the cookie is removed once the user quits his or her browser. As a result, specifying a date is a way for making a cookie survive across sessions. For this reason, cookies with expiration dates are referred to as "persistent" cookies.

72. Whenever a web browser loads a web page or component of a web page, it will include in its request for that component any cookies already stored on the user's computer that are associated with the domain hosting the content. The web server, in turn, can send a cookie or update a cookie already existing on the user's computer.

73. Upon each visit to a web site or a page within that site, a person's computer leaves certain electronic tracks or markers. Taken together, those markers create a trail of information commonly referred to as "clickstream data."

74. Clickstream data may include basic information, such as the type of computer an individual used to access the Internet, the kind of Internet browser utilized and the identification of each site or page visited. In addition, were an individual to disclose certain information during the visit, the clickstream data may

also include more personalized details, such as passwords, e-mail addresses, credit card numbers, name, address, date of birth, gender, or zip code.

75. Once an individual's hard drive contains a cookie for a particular Web site, each time a person navigates through that site and requests a different page, the server gains access to the current cookie text. In essence, the contents of the cookie file are attached to every subsequent request back to the server for a different webpage. Upon receiving the cookie contents that get embedded into the browser's request, the server may alter the cookie text to reflect new or updated information (such as the new page visited or any personal details disclosed on the page prior to sending the request). Along with the new page the user requested, the server would send a revised cookie file that replaces the old text. Thus, once deposited on a user's computer, cookies facilitate a flow of communication back and forth between an individual's computer and the server that maintains a website.

C. Web Browser Preferences

76. Computers are used for everything from banking and investing to shopping and communicating with others through email or chat programs. Although online communications may not be considered "top secret," online users do not want third parties reading their email, or examining personal information stored on their computer (such as financial statements), or downloading software, such as Flash cookies, without their knowledge or consent.

77. Individuals have a reasonable expectation of privacy in their personal computer, the integrity of their computers, and the confidentiality of their communications with the Internet websites that they visit, using their Internet connection to transmit and receive personal and private data, including but not limited to, personal emails, personal Internet research and viewing, credit card information, banking information, personal identifiable information such as social

security number, date of birth, and medical information.

78. Since some companies that used cookies have figured methods of tracking users when users visit various sites, most modern browsers allow users to set whether to allow or disallow HTML Cookies, by setting a browser to accept all cookies, to reject all cookies, or to notify you whenever a cookie is offered so that you can decide each time whether to accept it. When the user is prompted, the contents of the cookie can be viewed and the user can select whether to Deny, Allow for Session, or Allow the cookie. This gives the user more information about what sites are using cookies and also gives more granular control of cookies as opposed to globally enabling them.

79. Browser cookie controls and preference settings provide greater user privacy control. The purpose of a browser privacy mode is to allow users to browse the Internet without leaving data tracks. Browsers save visited websites in the browsing history, downloaded files in the download history, search terms in the search history, and data typed into online registration forms including cached version of such files. Cookie controls allow the user to decide which cookies can be stored on their computer and transmitted to websites, and using parental controls to block specific content by adjusting the tabs located within the user's browser.

80. Excluding the paragraph advanced by the advertising industry to promulgate questionable activities to the governmental authorities and privacy group, a majority of online users do not want tailored advertisements

> Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages - between 73% and 86% - say they would not want such advertising.

Turow, Joseph, King, Jennifer, Hoofnagle, Chris Jay, Bleakley, Amy and Hennessy, Michael, Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009). http://ssrn.com/abstract=1478214

D. Flash Player- Cookies-LSO

81. Flash Player is an application that, while running on a computer that is connected to the Internet, is designed to contemporaneously interact with websites containing Flash content that are being visited online. As such, under certain configurations, the application has the potential to silently compromise its users' Internet privacy, and do so without their knowledge. When stored on a user's computer, (.sol) files are capable of sending personally sensitive data back out over the Internet without the user's knowledge to one or more third parties.

82. Flash cookies are not transferred from the client back to the server like HTTP cookies. Instead, downloaded Flash objects that run locally in the web browser [locally stored/run objects] read and write these cookie-like files. Using JavaScript, this data can be pulled out of the Flash objects and then used like any other data by the web application. It is not necessary to have any visible signs that a Flash object is running on a given page. In fact, it would be difficult to reliably detect if an application were using Flash cookies. When you drill down in each domain's directory, you will eventually find a "SOL" file. This file contains the data that is stored and used as the Flash cookie.

83. DOM Storage is often compared to HTTP cookies. Like cookies, web developers can store per-session or domain-specific data as name/value pairs on the client using DOM Storage. However, unlike cookies, DOM Storage makes it easier to control how information stored by one window is visible to another.

84. Functionally, client storage areas are quite different from cookies. DOM Storage doesn't transmit values to the server with every request as cookies do, nor does the data in a local storage area ever expire. And unlike cookies, it is easy to access individual pieces of data using a standard interface that has growing support among browser vendors. If objects are stored in a Local Object Repository then these are available to specific actions but not to all the actions. But if these

objects are stored in one or more Shared Object Repositories then multiple actions or tests can use them.

85. A local shared-object can only be read the same domain that originates the shared object. Currently, using a local shared-object is the only way to instruct a Flash movie write data to the user's hard drive directly from within the movie. On Windows, local shared-objects are stored in Documents and Settings\userName\Application Data\Macromedia\Flash Player\#SharedObjects. According to the Macromedia docs, local shared-objects has a file extension of .SO, but saved with .SOL extension on Windows XP. Unlike cookies that are capable of storing only text values, Local Shared Objects can store many data types including Number, String, Boolean, XML, Date, Array, and Object.

86. Flash LSO cookies properties:

- SOL files are stored outside of the browser's cache, and removed when a web browser's cache is cleared.
- By default they offer storage of 100 KB (compare: Usual cookies 4 KB).
- Browsers are not aware of Flash cookies, and LSO's usually cannot be removed by browsers.
- Flash can access and store highly specific personal and technical information (system, user name, files...).
- Ability to send the stored information to the appropriate server, without user's permission.
- Flash applications do not need to be visible
- There is no easy way to tell which Flash-cookie sites are tracking you.
- Shared folders allow cross-browser tracking
- There is currently no mechanism to force a shared-object to "expire". Browser cookies have an expiration mechanism built in.
- User can only disable local shared-object by disallowing a particular site to write to the user's hard drive. This can be done in the Macromedia player Setting window.

87. Since Flash runs independently from the browser, it needs its own temporary storage area for web sites to store information related to the Flash movie, saving objects, in either the local and shared object repositories. The data is split into two folders: "#SharedObjects" and "macromedia.com". The content located inside the "macromedia.com" is set by the site and controls settings for the site visited, while the content located inside "#SharedObjects" is created by the site

visited or a third party company and contains the cookie values we are researching.

88. Defendants' Flash cookie setting process was a system, method and computer readable medium configured to track Internet users as they browse web-sites when cookies are disabled or deleted. Defendant Clearspring Flash Cookie Affiliate's website receives a request for content from the computing-device. After obtaining information about the computing-device, the tracking-server assesses the request for content from the computing-device. If the computing-device has an available Flash plug-in, the tracking-server transmits a Flash applet to the computing-device. The Flash applet is configured to: determine whether a unique Flash identifier has been assigned to the computing-device, generate the unique Flash identifier if no unique Flash identifier has already been assigned to the computing-device, transmit the unique Flash identifier to a tracking server, and store the unique Flash identifier in local Flash storage. The process also stores a cookie at the computing-device when no Flash plug-in is available.

E. "Flash Cookies and Privacy"- Berkeley Study

89. A study released by researchers at the University of California, Berkeley and other universities, submitted to the federal government for consideration as part of a new policy on the use of tracking technologies, revealed the details of Defendant Clearspring's online privacy invasion of epidemic proportions, that reverberated globally.

> Ashkan Soltani *et al.*, "Flash Cookies and Privacy" (10 August 2009), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

F. Overlapping Values

90. The "Flash Cookies and Privacy," study attempted to infer the intended uses of particular Flash cookies by examining the variable name for each cookie, *i.e.*, volume, userID, and user, referred to as a "unique identifier;"

> *It's also worth mentioning that '_tpf' and '_fpf' were found to also contain unique identifiers which were also found to contain*

> *overlapping values as the ones found in HTML cookies for 'uid' or 'userid.'"*
>
> *"Of the top 100 websites, 31 had at least one overlap between a HTTP and Flash cookie. For instance, a website might have an HTTP cookie labeled "uid" with a long value such as 4a7082eb-775d6-d440f-dbf25. There were 41 such matches on these 31 sites. Most Flash cookies with matching values were served by third-party advertising networks. That is, upon a visit to a top 100 website, a third party advertising network would set both a third party HTTP cookie and a third party Flash cookie.*

Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, Chris Jay Hoofnagle, "Flash Cookies and Privacy" (10 August 2009), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

91. "Zombie cookies," or browser cookies that are respawned by Flash cookies, required a Flash setting file and a directory, labeled by the domain, which set the Flash cookie. Such created a history of all users' activities, thus the coding required was neither inadvertent nor an "unintended effect," and permitted the Flash cookie to respawn a deleted browser cookie derived from the history data file:

> *Presence of Flash settings files- Each settings is stored in its own directory, labeled by domain. This creates a type of history file parallel to the one created by the browser. However, the Flash history is not deleted when browser controls are used to erase information about sites previously visited. This means that uses may falsely believe that they have fully cleared their history when using the standard browser tools."*
>
> Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, Chris Jay Hoofnagle, "Flash Cookies and Privacy" (10 August 2009), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

92. A technical discussion alone of respawning Flash cookies by ad networks in general, without visualization of such activity, fails to accentuate the willful and wanton disregard of user's preferences. Case in point: User's preference is to opt-out from having a Flash cookie set, this on 3/21/2010 at 10:18:08 AM evidenced within the log activity as "optout.sol."

> http://core. [name redacted].com/#com/[name redacted]OptOut.sol 3/21/2010 10:18:08 AM 3/21/2010 10:18:08 AM 61 C:\Users\[user's name redacted] \AppData\Roaming\Macromedia\Flash Player\#SharedObjects\3VYPQS2K\core. [name redacted].com\#com\[name redacted]\OptOut.sol

93. User's Flash cookie preference is disregarded as evidenced within the log activity as "retargeting.sol." Such activity occurs within five (5) second on 3/21/2010 10:18:13 AM.

> http://core.[name redacted].com/#com/[name redacted].
> Retargeting.sol 3/21/2010 10:18:13 AM 5/22/2010 9:12:24 AM
> 120 C:\Users\[user's name redacted]
> \AppData\Roaming\Macromedia\Flash
> Player\#SharedObjects\3VYPQS2K\core. [name
> redacted].com\#com\[name redacted].\Retargeting.sol

94. The expiration date of cookie information and the entropy of the information contained in the cookie provides limited information. If the entropy is low (e.g. content is "volume =5") then it can be assumed to be a legitimate setting to be saved. If the entropy is high (e.g. "userId = b56574ce78d2f110b1gd522") then it is more likely than not a tracking id connected to a background database of user information, i.e. a user goes to a website wherein the algorithm locates a normal cookie stored by an advertising network, then the algorithm searched for repeating keys. Every character (at least in a charset like ASCII) counts one byte, thus counting the number of characters in "id=344499284532" which are 15 and in "volume_level=98, language=English" which are 32. The analysis of both HTTP and Flash cookies for key identifiers revealed undisputable correlations including overlapping values.

95. Researchers were able to indentify a high number of cookies similarly labeled such as: "user ID." These cookies stored unique identifiers which allowed user tracking; however unlike HTTP cookies used for tracking these cookies had overlapping values. This respawning was because of the Flash cookies, provided by Clearspring, had the same data values as the HTTP cookies, provided by the Clearspring Flash Cookie Affiliates, so in effect the Flash cookies acted as a back-up on the computer systems once the HTTP cookies had been removed. If users simply deleted cookies without clearing the browser cache, the identifiers in the

deleted browser cookies still returned to the cookies, more than likely, using information stored in the cache.

96. When HTML cookies are deleted, the users would get a new value when visiting the site. But when Flash cookies and HTML cookies are given the same value, as they were on 31 of the top 100 websites, "it will restore the value of your original cookie, and thereby nullifies the deletion of the HTML cookies," Soltani said

> Moscaritolo, Angela. " Top Websites using Flash cookies to track user behavior." *SC Magazine*. (August 11, 2009) http://www.scmagazineus.com/top-websites-using-Flash-cookies-to-track-user-behavior/article/141486/

97. Defendants implanted identical code in the Plaintiffs and Class Members' computers resulting in a uniform action to set redundant unique identifiers used to identify and track users overlapping values.

G. Defendants' Harmful Business Practices

98. Defendant Clearspring's activities with Clearspring Flash Cookie Affiliates occurred throughout the United States, and have secretly obtained personal and private information from Plaintiffs and the Class - a course of action and a body of information that is protected from interception, access, and disclosure by federal law.

99. Defendant used, interfered with, and intermeddled with Class Members' ownership of their personal property, namely, their computers, by, directly or indirectly, secretly depositing cookies on their computers, secretly accessing their computers to obtain information contained in and enabled by the cookie, and secretly collecting personal data and information regarding each Class Members' Internet surfing habits contained in electronic storage on his/her computer.

100. At all relevant times, Defendants' advertising technology has

contained secret information-gathering capacities that were not disclosed to or known by Plaintiffs or the Class and which permitted Defendants to surreptitiously, in an unauthorized manner, and for tortious and unlawful purposes, intercept and access Plaintiffs' and the Class Members' personal and private information, monitor their Internet activity, and create detailed personal profiles based on such information.

101. At all relevant times, Plaintiffs and the Class, as part of their normal Internet browsing and usage, visited websites that, unbeknownst to them, and Defendant utilized and/or facilitated tracking and profiling technology. Since they were doing so in the privacy of their own homes or offices, and since Defendant did not display any warning or indication that it was collecting or transmitting personal and private information to or from their computer systems, Plaintiffs and the Class had a reasonable expectation of privacy as to the nature of their activity and the contents of any information they provided to or obtained from a particular website.

102. Defendants have used those cookies and other surreptitious data-collection methods to secretly intercept and access computer users' personal data and web browsing habits and have transmitted this information to Defendants for their own commercial benefit.

103. Defendants collected and/or disclosed covered information of Class Members about all or substantially all of their online activity, including across websites.

104. Defendants' business practice unfairly wrests control from users who choose to delete their cookies in order to avoid being tracked. Advertising networks use unique IDs to identify the same user or computer across many different websites. Users who are aware of this may delete their cookies periodically, believing that the new cookies they receive will contain new unique identifiers, thus hindering the ability of advertising networks to track their behavior

across sites. Using Flash cookies to re-identify users overrides this control, with little available redress for users. Although users may arguably protect themselves by periodically deleting their Flash cookies as well, the means for doing so are extremely obscure and difficult even for savvy consumers to use. Flash specifically attempts to obfuscate data within each LSO by controlling the format and forcing a binary serialization of any stored data, thus bypassing the web browser's same-origin security policy, allowing an application hosted on one domain to read data or code hosted on another.

105. Defendants failed to disclose that its applied technologies also provide Defendants with the ability to surreptitiously intercept, access, and collect electronic communications and information from unsuspecting Internet users—including Plaintiffs and the Class.

106. Defendants intercepted Class Members' electronic communications for the purpose of committing a tortious or criminal act, and violated the constitutional rights of Plaintiffs and Class Members.

107. In all cases where some notice was provided, that notice was insufficient, misleading, and inadequate. Consent under such circumstances was impossible.

108. In no case as alleged in this complaint, was adequate, informed notice provided to any Class Member of the true nature and function of the Defendant service.

109. In any case where the opportunity of 'opting out' of the Defendant service was provided, such 'opt out' rights were misleading, untrue, and deceptive.

110. In no case was the collection of all Internet communication data between the consumer and the Internet halted or affected in any way. All data was still collected. The 'opt out' only affected what advertisements the consumer was shown. Thus, the provision of the opportunity for opting out was, itself, totally misleading.

111. Plaintiffs and the Class Members did not voluntarily disclose their personal and private information, including their Internet surfing habits, to Defendants - and indeed never even knew that Defendants existed or conducted data collection and monitoring activities upon and across its clients' websites. Plaintiffs and the Class Members provided such information, and had their Internet habits monitored, without their knowledge or consent, and would not have consented having their personal and private information, including their on-line profiles, used for Defendants' commercial gain.

112. Defendants did not obtain consent from Plaintiffs and Class Members for any collection or use and was not allowed to decline consent at the time such statement was presented to the Class Members.

113. Defendants did not obtain consent from Plaintiffs and Class Members for any disclosure of covered information to unaffiliated parties and was not allowed to decline consent at the time such statement was presented to the Class Members.

114. Defendants have covertly, without consent, and in an unauthorized, deceptive, invasive, and fraudulent manner implanted Internet "Flash cookies" upon Internet users' computer hard disk drives to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.

115. Defendant intentionally accessed Plaintiffs and Class Members' computer without authorization or exceeded authorized access to obtain information from a protected computers, involved an interstate communications.

116. Defendants sold, shared, and/or otherwise disclosed covered information of Class Members to an unaffiliated party without first obtaining the consent of the Class Members to whom the covered information related to.

117. At all relevant times, Plaintiffs and Class Members' personal and private information was intercepted by and/or accessed by Defendants and

transmitted to it on a regular basis, without alerting Internet users in any manner. As a result, Defendants were able to and did access Plaintiffs' and Class Members' computer systems and/or intercept their electronic communications without authorization. Defendants have obtained, compiled, and used this personal information for its own commercial purposes.

118. Defendants intercepted Class Members' electronic communications for the purposes of implanting unauthorized Flash cookies on Class Members' computers; repeatedly accessing electronic communications without Class Members' knowledge and consent so as to profile such persons' web browsing habits, secretly tracking Class Members' activities on the Internet and collecting personal information about consumers; and profiting from the use of the illegally obtained information, all to Defendants' benefit and Class Members' detriment.

119. Defendants intentionally intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept the electronic communication of Plaintiffs and Class Members.

120. Defendants have, either directly or by aiding, abetting and/or conspiring to do so, knowingly, recklessly, or negligently disclosed, exploited, misappropriated and/or engaged in widespread commercial usage of Plaintiffs' and the Class' private and sensitive information for defendants' own benefit without Plaintiffs' or the Class' knowledge, authorization, or consent. Such conduct constitutes a highly offensive and dangerous invasion of Plaintiffs' and the Class' privacy.

121. Defendants used and consumed the resources of the Plaintiffs and Class Members' computers and substantially increased their Internet bandwidth by gathering user information and transferring such to Defendants.

122. Defendants caused harm and damages to Plaintiffs and Class Members' computers finite resources, depleted and exhausted its memory, thus causing an actual inability to use it for its intended purposes, and significant

unwanted CPU activity, disk usage, and network traffic resulting in instability issues, such as applications freezing, failure to boot, and system-wide crashes.

123. Defendants caused harm and damages to the Plaintiffs and Class Members including but not limited to, consumption of their device's finite resources, memory depletion which resulted in the actual inability to use if for its intended purposes.

124. The cumulative effect, and the interactions between spyware components, caused the symptoms commonly reported by users: "a computer, which slows to a crawl," or "overwhelmed by the many processes running on it."

125. Defendants' downloads were not evident. Users assumed that the issues relate to hardware, Windows installation problems, or another infection, and resorted to contacting technical support experts, or even buying a new computer because the existing system "has become too slow." Class Members attempting to repair their own computer risked damaging their system files. Badly infected systems required a clean reinstallation of all their software in order to return to full functionality, with charges of a few hundred dollars to remove viruses and spyware, and unauthorized Flash cookies, if serviced in house, or on site such costs exceeded $40-$60 per hour.

126. Defendants harmed Plaintiffs and Class Members by its actions which included, but not limited to the following:

a) Loss of valuable data by attempts to remove Flash cookies once discovered;

b) Incurred economic losses accompanied by an interruption in service;

c) Functionality of computer interfered with, including an inability of websites visited once Flash content was disabled;

d) Information was deleted, otherwise made unavailable;

e) Impaired the integrity and availability of data, programs and information.

127. Defendants' technology wrongfully monitored Internet users' activities at each and every website users visited at which Defendants' products or services were not utilized. The wrongfulness of this conduct is multiplied by the fact that Defendants aggregate this information about users' habits across numerous websites and unjustly enriched defendant to the severe detriment of Plaintiffs and the Class. Plaintiffs and the Class have been harmed, as they have been subjected to repeated and unauthorized invasions of their privacy - violations which continue to this day.

CLASS ALLEGATIONS
Allegations as to Class Certification

128. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this action as a Class action, on behalf of themselves and all others similarly situated as members of the following Classes (collectively, the "Class"):

a) U.S. Resident Class: All persons residing in the United States that accessed a Clearspring Flash Cookie Affiliate website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.

b) California Resident Class: All persons residing in California that accessed a Clearspring Flash Cookie Affiliate website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later. All California Resident Class Members are also members of the U.S. Resident Class.

c) Injunctive Class: All persons after the date of the filing of this complaint, residing in the United States, that accessed a Clearspring Flash Cookie Affiliate website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.

129. The Class action period, (the "Class Period"), pertains to the date, two years preceding the date of this filing to the date of Class certification, that a

person residing in the United States, that accessed a Clearspring Flash Cookie Affiliate website, and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.

130. Plaintiffs reserve the right to revise this definition of the Class based on facts learned in the course of litigation of this matter.

131. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this Class action, on behalf of themselves and the following Classes with respect to Plaintiffs' claims for violation of the:

a) Computer Fraud and Abuse Act ("CFAA"),

b) California's Computer Crime Law, ("CCCL"),

c) Trespass to Personal Property / Chattels, and

d) Unjust Enrichment against *ALL DEFENDANTS*:

> All persons residing in United States who, during the period of two years preceding the date of this filing to the date of Class certification (the "Class Period"), accessed a Clearspring Flash Cookie Affiliate website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.
> (hereinafter referred to as "CFAA/ ECPA/CCCL SubClass.")

132. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this Class action, on behalf of themselves and the following Class with respect to Plaintiffs' claims for violation of the:

a) California's Computer Crime Law ("CCCL"),

b) California's Invasion of Privacy Act, against *DEFENDANT CLEARSPRING, ALONE*:

> All persons residing in United States who, during the Class period, and accessed a Clearspring Flash Cookie Affiliate website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.
> (hereinafter referred to as "Clearspring SubClass.")

133. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this Class action, on behalf of themselves and the following Class with respect to Plaintiffs' claims for violation of the:

a) California's Invasion of Privacy Act, against DEFENDANTS *DEMAND MEDIA, DISNEY, PROJECT PLAYLIST, SOAPNET, SODAHEAD, and USTREAM* (hereinafter referred to as "California Defendants"):

> All persons residing in United States who, during the Class period, and accessed one or more of the California Defendants' website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.
> (hereinafter referred to as "California Defendants SubClass")

134. On behalf of the U.S. Resident and California Resident Classes, Plaintiffs seek equitable relief, damages and injunctive relief pursuant to:

a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

b) California's Computer Crime Law, Penal Code § 502;

c) California Invasion Of Privacy Act, California Penal Code § 630;

d) Trespass to Personal Property / Chattels;

e) Unjust Enrichment

135. On behalf of the Injunctive Class, Plaintiffs seek only injunctive relief.

136. **Persons Excluded From Classes:** Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint. Specifically excluded from the proposed Class are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants and/or their officers and/or directors, or any of

them; the Judge assigned to this action, and any member of the Judge's immediate family.

137. Plaintiffs reserve the right to revise these Class definitions of the Classes based on facts they learn during discovery.

138. **Numerosity:** The members of the Class are so numerous that their individual joinder is impracticable. Plaintiffs are informed and believe, and on that basis allege, that the proposed Class contains tens of thousands of members. The precise number of Class Members is unknown to Plaintiffs. The true number of Class Members is known by Defendants, however and, thus, Class Members may be notified of the pendency of this action by first Class mail, electronic mail, and by published notice. Upon information and belief, Class Members can be identified by the electronic records of defendants.

139. **Class Commonality:** Pursuant to Federal Rules of Civil Procedure, Rule 23(a)(2) and Rule *23(b)(3)*, are satisfied because there are questions of law and fact common to Plaintiffs and the Class, which common questions predominate over any individual questions affecting only individual members, the common questions of law and factual questions include, but are not limited to:

a) What was the extent of Clearspring and Clearspring Flash Cookie Affiliates' business practice of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later and how did it work?

b) What information did Clearspring and Clearspring Flash Cookie Affiliates' collect from its business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later, and what did it do with that information?

c) Whether Clearspring Flash Cookie Affiliate users, by virtue of their visitation to Clearspring Flash Cookie Affiliate's website, had pre-consented to the operation of Clearspring and Clearspring Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later;

d) Was there adequate notice, or *any* notice, of the operation of Clearspring and Clearspring Flash Cookie Affiliates' business

practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later provided to Clearspring and Clearspring Flash Cookie Affiliates' users?

e) Was there reasonable opportunity to decline the operation of Clearspring and Clearspring Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later provided to Clearspring and Clearspring Flash Cookie Affiliates' users?

f) Did Clearspring and Clearspring Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later disclose, intercept, and transmit personally identifying information, or sensitive identifying information, or personal information?

g) Whether Clearspring and Clearspring Flash Cookie Affiliates devised and deployed a scheme or artifice to defraud or conceal from Plaintiffs and the Class Clearspring and Clearspring Flash Cookie Affiliates' ability to, and practice of, intercepting, accessing, and manipulating, for its own benefit, personal information, and tracking data from Plaintiffs' and the Class' personal computers via the ability to; (and practice of) implanting secret "cookies" on their computers;

h) Whether Clearspring and Clearspring Flash Cookie Affiliates engaged in deceptive acts and practices in, connection with its undisclosed and systemic practice of implanting, accessing and/or disclosing unique identifiers, tracking data, and personal information on Plaintiffs and the Class' personal computers and using that data to track and profile Plaintiffs' and the Class' Internet activities and personal habits, proclivities, tendencies, and preferences for defendants' use and benefit;

i) Did the implementation of Clearspring and Clearspring Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030?

j) Did the operation, function, and/or implementation of Clearspring and Clearspring Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later violate California's Computer Crime Law, California Penal Code § 502?

k) Did the operation, function, and/or implementation of Clearspring and Clearspring Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later violate the California Invasion of

Privacy Act, California Penal Code § 630?

l) Did the operation, function, and/or implementation of Clearspring and Clearspring Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later unjustly enrich the Defendants herein?

m) Are the Defendants Clearspring and/or Clearspring Flash Cookie Affiliates liable under a theory of aiding and abetting for violations of the statutes listed herein?

n) Are the Defendants Clearspring and/or Clearspring Flash Cookie Affiliates liable under a theory of civil conspiracy for violations of the statutes listed herein?

o) Are the Defendants Clearspring and/or Clearspring Flash Cookie Affiliates liable under a theory of unjust enrichment for violations of the statutes listed herein?

p) Whether Clearspring and Clearspring Flash Cookie Affiliates participated in and/or committed or is responsible for violation of law(s) complained of herein;

q) Are Class Members entitled to damages as a result of the implementation of Clearspring and Clearspring Flash Cookie Affiliates' marketing scheme, and, if so, what is the measure of those damages?

r) Whether Plaintiffs and members of the Class have sustained damages as a result of Defendants' conduct, and, if so, what is the appropriate measure of damages;

s) Whether Plaintiffs and members of the Class are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

t) Whether Plaintiffs and members of the Class are entitled to punitive damages, and, if so, in what amount.

140. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class in that Plaintiffs and each member of the Class accessed a Clearspring Flash Cookie Affiliate website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.

141. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained counsel

highly experienced in complex consumer Class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

142. **Superiority:** A Class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against the Defendants. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if Class Members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the Class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

143. In the alternative, the Class may be also certified because:

a) the prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudication with respect to individual Class Members that would establish incompatible standards of conduct for the Defendants;

b) the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

c) Defendants have acted or refused to act on grounds generally applicable to the Class thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

144. The claims asserted herein are applicable to all persons throughout the United States that accessed a Clearspring Flash Cookie Affiliate website and a Flash cookie was set on their computer to use its local storage within the Flash media player to back up browser cookies for the purposes of restoring them later.

145. The claims asserted herein are based on Federal law and California law, which is applicable to all Class Members throughout the United States.

146. Adequate notice can be given to Class Members directly using information maintained in Defendants' records, or through notice by publication.

147. Damages may be calculated from the information maintained in Defendants' records, so that the cost of administering a recovery for the Class can be minimized. The amount of damages is known with precision from Defendants' records.

Count I
Violation of the Computer Fraud and Abuse Act
18 U.S.C. § 1030 *et seq.*
Against All Defendants

148. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

149. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

150. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and relates activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

151. Defendants violated 18 U.S.C. § 1030 by intentionally accessing a Plaintiffs' computer, without authorization or by exceeding access, thereby

obtaining information from such a protected computer.

152. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), provides a civil cause of action to "any person who suffers damage or loss by reason of a violation" of CFAA.

153. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)(i), makes it unlawful to "knowingly cause[s] the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause[s] damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

154. Plaintiffs' computer is a "protected computer...which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

155. Defendants violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing a Plaintiffs' computer, without authorization or by exceeding access, thereby obtaining information from such a protected computer.

156. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a command embedded within their webpages, downloaded to Plaintiffs' computer, which are protected computers as defined in 18 U.S.C. § 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs' viewing habits, Defendants intentionally caused damage without authorization to those Plaintiffs' computers by impairing the integrity of the computer.

157. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs and Class Members' protected computers without authorization, and as a result of such conduct, recklessly caused damage to Plaintiffs and Class Members' computers by impairing the integrity of data and/or system and/or information.

158. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally accessing Plaintiffs and Class Members' protected computers without

authorization, and as a result of such conduct, caused damage and loss to Plaintiffs and Class Members.

159. Plaintiffs have suffered damage by reason of these violations, as defined in 18 U.S.C. § 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

160. Plaintiffs have suffered loss by reason of these violations, as defined in 18 U.S.C. § 1030(e)(11), by the "reasonable cost ... 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."

161. Plaintiffs have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, disclosure of personal indentifying information, sensitive identifying information, and personal information, interception, and transactional information that otherwise is private, confidential, and not of public record.

162. As a result of these takings, Defendants' conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

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

164. Defendants' unlawful access to Plaintiffs' computers and electronic communications has caused Plaintiffs irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

Count II
Violation of California's Computer Crime Law ("CCCL")
California Penal Code § 502
Against All Defendants

165. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

166. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

167. The California Computer Crime Law, California Penal Code § 502, referred to as "CCCL" regulates "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."

168. Defendants violated California Penal Code § 502 by knowingly accessing, copying, using, made use of, interfering, and/or altering, data belonging to Plaintiffs and Class Members: (1) in and from the State of California; (2) in the home states of the Plaintiffs; and (3) in the state in which the servers that provided the communication link between Plaintiffs and the websites they interacted with were located.

169. Pursuant to California Penal Code § 502(b)(1), "Access means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network."

170. Pursuant to California Penal Code § 502(b)(6), "Data means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device."

171. Pursuant to California Penal Code § 502(b)(8), "Injury means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to

legitimate users of a computer system, network, or program."

172. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network."

173. Defendants have violated California Penal Code § 502(c)(1) by knowingly accessing and without permission, altering, and making use of data from Plaintiffs' computers in order to device and execute business practices to deceive Plaintiffs and Class Members into surrendering private electronic communications and activities for Defendants' financial gain, and to wrongfully obtain valuable private data from Plaintiffs.

174. Defendants have violated California Penal Code § 502(c)(2) by knowingly accessing and without permission, taking, or making use of data from Plaintiffs' computers.

175. Defendants have violated California Penal Code § 502(c)(3) by knowingly and without permission, using and causing to be used Plaintiffs' computer services.

176. Defendants have violated California Penal Code § 502(c)(4) by knowingly accessing and without permission, adding and/or altering the data from Plaintiffs' computers.

177. Defendants have violated California Penal Code § 502(c)(5) by knowingly and without permission, disrupting or causing the disruption of

Plaintiffs' computer services or denying or causing the denial of computer services to Plaintiffs.

178. Defendants have violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' computers, computer system, and/or computer network.

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

180. Defendants have violated California Penal Code § 502(c)(8) by knowingly introducing a computer contaminant into the Plaintiffs' computer, computer system and/or computer network to obtain data regarding Plaintiffs' electronic communications.

181. California 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."

182. Plaintiffs have also suffered irreparable injury from these unauthorized acts of disclosure, to wit: all of their personal, private, and sensitive electronic communications have been harvested, viewed, accessed, stored, and used by Defendants, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, entitling Plaintiffs to injunctive relief.

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

184. As a direct and proximate result of Defendants' unlawful conduct within the meaning of California Penal Code § 502, Defendants have caused loss

to Plaintiffs in an amount to be proven at trial. Plaintiffs are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

185. Plaintiffs and the Class Members seek compensatory damages, in an amount to be proven at trial, and injunctive or other equitable relief.

186. Plaintiffs and Class Members have suffered irreparable and incalculable harm and injuries from Defendants' violations. The harm will continue unless Defendants are enjoined from further violations of this section. Plaintiffs and Class Members have no adequate remedy at law.

187. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendants' violation were willful and, on information and belief, Defendants are guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

188. Defendants' unlawful access to Plaintiffs' computers and electronic communications has caused Plaintiffs irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs to remedies including injunctive relief as provided by California Penal Code § 502(e).

Count III
Violation of the California Invasion of Privacy Act
Penal Code section 630 et seq.
Against Clearspring, Walt Disney Internet Group, Demand Media, Project Playlist, Soapnet, SodaHead, Ustream, and Warner Bros. Records, (hereinafter "California Defendants")

189. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

190. Plaintiffs assert this claim against each and every California Defendant named herein in this complaint on behalf of themselves and the Class.

191. California Penal Code section 630 provides, in part:

> Any person who, . . . or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . .

192. On information and belief, each Plaintiff and each Class Member, during one or more of their interactions on the Internet during the Class period, communicated with one or more web entities based in California, or with one or more entities whose servers were located in California.

193. Communications from the California web-based entities to Plaintiffs and Class Members were sent from California. Communications to the California web-based entities from Plaintiffs and Class Members were sent to California.

194. Plaintiffs and Class Members did not consent to any of the Defendants' actions in intercepting, reading, and/or learning the contents of their communications with such California-based entities.

195. Plaintiffs and Class Members did not consent to any of the Defendants' actions in using the contents of their communications with such California-based entities.

196. Defendants are not a "public utility engaged in the business of providing communications services and facilities . . ."

197. The actions alleged herein by the Defendants were not undertaken: "for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility."

198. The actions alleged herein by the Defendants were not undertaken in

connection with: "the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility."

199. The actions alleged herein by the Defendants were not undertaken with respect to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

200. The Defendants directly participated in the interception, reading, and/or learning the contents of the communications between Plaintiffs, Class Members and California-based web entities.

201. Alternatively, and of equal violation of the California Invasion of Privacy Act, the Defendants aided, agreed with, and/or conspired with Clearspring to unlawfully do, or permit, or cause to be done all of the acts complained of herein.

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

203. Unless restrained and enjoined, Defendants will continue to commit such acts. Pursuant to Section 637.2 of the California Penal Code, Plaintiffs and the Class have been injured by the violations of California Penal Code section 631. Wherefore, Plaintiffs, on behalf of themselves and on behalf of a similarly situated Class of consumers, seek damages and injunctive relief.

COUNT IV
Violations of the Consumer Legal Remedies Act ("CLRA") California Civil Code § 1750, et seq.
Against All Defendants

204. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

205. In violation of Civil Code section 1750, et seq. (the "CLRA"), Defendant has engaged and is engaging in unfair and deceptive acts and practices

in the course of transactions with Plaintiffs, and such transactions are intended to and have resulted in the sales of services to consumers. Plaintiffs and the Class Members are "consumers" as that term is used in the CLRA because they sought or acquired Defendants' good or services for personal, family, or household purposes. Defendants' past and ongoing acts and practices include but are not limited to:

a) Defendants' representations that their services have characteristics, uses, and benefits that they do not have, in violation of Civil Code § 1770(a)(5);

b) Defendants' representations that their services are of a particular standard, quality and grade but are of another standard quality and grade, in violation of Civil Codes § 1770(a)(7); and

c) Defendants' advertisement of services with the intent not to sell those services as advertised, in violation of Civil Code § 1770(a)(9).

206. Defendants' violations of Civil Code § 1770 have caused damage to Plaintiffs and the other Class Members and threaten additional injury if the violations continue. This damage includes the losses set forth above.

207. At this time, Plaintiffs seek only injunctive relief under this cause of action. Pursuant to California Civil Code, Section 1782, Plaintiffs will notify Defendants in writing of the particular violations of Civil Code, Section 1770 and demand that Defendants rectify the problems associated with their behavior detailed above, which acts and practices are in violation of Civil Code § 1770.

208. If Defendants fails to respond adequately to Plaintiffs' above described demand within 30 days of Plaintiffs' notice, pursuant to California Civil Code, Section 1782(b), Plaintiffs will amend the complaint to request damages and other relief, as permitted by Civil Code, Section 1780.

COUNT V
Violations of the Unfair Competition Law ("UCL") California Business and Professions Code § 17200, et seq.
Against All Defendants

209. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

210. In violation of California Business and Professions Code § 17200 et seq., Defendants' conduct in this regard is ongoing and includes, but is not limited to, unfair, unlawful and fraudulent conduct.

211. By engaging in the above-described acts and practices, Defendants have committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs and the Class have suffered injury-in-fact and have lost money and/or property—specifically, personal information and/or registration fees.

212. Defendants' business acts and practices are unlawful, in part, because they violate California Business and Professions Code § 17500, et seq., which prohibits false advertising, in that they were untrue and misleading statements relating to Defendants' performance of services and with the intent to induce consumers to enter into obligations relating to such services, and regarding statements Defendants knew were false or by the exercise of reasonable care Defendants should have known to be untrue and misleading.

213. Defendants' business acts and practices are also unlawful in that they violate the California Consumer Legal Remedies Act, California Civil Code, Sections 1647, et seq., 1750, et seq., and 3344, California Penal Code, section 502, and Title 18, United States Code, Section 1030. Defendants are therefore in violation of the "unlawful" prong of the UCL.

214. Defendants' business acts and practices are unfair because they cause harm and injury-in-fact to Plaintiffs and Class Members and for which Defendants

has no justification other than to increase, beyond what Defendants would have otherwise realized, their profit in fees from advertisers and their information assets through the acquisition of consumers' personal information. Defendants' conduct lacks reasonable and legitimate justification in that Defendants have benefited from such conduct and practices while Plaintiffs and the Class Members have been misled as to the nature and integrity of Defendants' services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendants' conduct offends public policy in California tethered to the Consumer Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to obtain material information that enables them to safeguard their own privacy interests, including California Civil Code, Section 1798.80.

215. In addition, Defendants' modus operandi constitutes a sharp practice in that Defendants knew, or should have known, that consumers care about the status of personal information and email privacy but were unlikely to be aware of the manner in which Defendants failed to fulfill their commitments to respect consumers' privacy. Defendants are therefore in violation of the "unfair" prong of the UCL.

216. Defendants' acts and practices were fraudulent within the meaning of the UCL because they are likely to mislead the members of the public to whom they were directed.

Count VI
Trespass to Personal Property / Chattels
Against All Defendants

217. Plaintiffs incorporate by reference and reallege all paragraphs previously alleged herein.

218. The common law prohibits the intentional intermeddling with personal property, including a computer, in possession of another that results in the deprivation of the use of the personal property or impairment of the condition,

quality, or usefulness of the personal property.

219. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiffs and Class Members, Defendants dispossessed Plaintiffs and Class Members from use and/or access to their computers, or parts of them. Further, these acts impaired the use, value, and quality of Plaintiffs' and Class Members' computers. Defendants' acts constituted an intentional interference with the use and enjoyment of the computers. By the acts described above, Defendants have repeatedly and persistently engaged in trespass to personal property in violation of the common law.

220. Without Plaintiffs' and Class Members' consent, or in excess of any consent given, Defendants knowingly and intentionally accessed Plaintiffs' and Class Members' property, thereby intermeddling with Plaintiffs' and Class Members' right to possession of the property and causing injury to Plaintiffs and the members of the Class.

221. Defendants engaged in deception and concealment in order to gain access to Plaintiffs and Class Members' computers.

222. Defendants undertook the following actions with respect to Plaintiffs' and Class Members' computer:

a) Defendants accessed and obtained control over the user's computer;

b) Defendants caused the installation of a new code onto the hard drive of the user's computer;

c) Defendants programmed the operation of its code to function and operate without notice or consent on the part of the owner of the computer, and outside of the control of the owner of the computer.

223. All these acts described above were acts in excess of any authority any user granted when he or she visited the Clearspring Flash Cookie Affiliates'

websites and none of these acts was in furtherance of users viewing the Clearspring Flash Cookie Affiliates websites. By engaging in deception and misrepresentation, whatever authority or permission Plaintiffs and Class Members may have granted to Clearspring Flash Cookie Affiliates was vitiated.

224. Defendants' installation and operation of its program used, interfered, and/or intermeddled with Plaintiffs' and Class Members' computer systems. Such use, interference and/or intermeddling was without Class Members' consent or, in the alternative, in excess of Plaintiffs' and Class Members' consent.

225. Defendants' installation and operation of its program constitutes trespass, nuisance, and an interference with Class Members' chattels, to wit, their computers.

226. Defendants' installation and operation of its program impaired the condition and value of Class Members' computers.

227. Defendants trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and Class Members.

228. As a direct and proximate result of Defendants' trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiffs' and Class Members' property, Defendants has injured and impaired in the condition and value of Class Members' computers, as follows:

a) By consuming the resources of and/or degrading the performance of Plaintiffs' and Class Members' computers (including hard drive space, memory, processing cycles, and Internet connectivity);

b) By diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiffs' and Class Members' computers;

c) By devaluing, interfering with, and/or diminishing Plaintiffs' and Class Members' possessory interest in their computers;

d) By altering and controlling the functioning of Plaintiffs' and Class Members' computers;

e) By infringing on Plaintiffs' and Class Members' right to exclude others from their computers;

f) By infringing on Plaintiffs' and Class Members' right to determine, as owners of their computers, which programs should be installed and operating on their computers;

g) By compromising the integrity, security, and ownership of Class Members' computers; and

h) By forcing Plaintiffs and Class Members' to expend money, time, and resources in order to remove the program installed on their computers without notice or consent.

Count VII
Unjust Enrichment
Against All Defendants

229. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

230. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

231. A benefit has been conferred upon all defendants by Plaintiffs and the Class. On information and belief, Defendants, directly or indirectly, have received and retain information regarding online communications and activity of Plaintiffs, and Defendants have received and retain information regarding specific purchase and transactional information that is otherwise private, confidential, and not of public record, and/or have received revenue from the provision of such information.

232. Defendants appreciate or have knowledge of said benefit.

233. Under principles of equity and good conscience, Defendants should not be permitted to retain the information and/or revenue which they acquired by

virtue of their unlawful conduct. All funds, revenues, and benefits received by Defendants rightfully belong to Plaintiffs and the Class, which Defendants have unjustly received as a result of its actions.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, prays for judgment against Defendants as follows:

A. Certify this case as a Class action on behalf of the Classes defined above, appoint Plaintiffs as Class representatives, and appoint their counsel as Class counsel;

B. Declare that the actions of Clearspring and Clearspring Flash Cookie Affiliates, as set out above, violate the following:

a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
b) California's Computer Crime Law, Penal Code § 502;
c) California's Invasion Of Privacy Act, California Penal Code § 630;
d) California's Consumer Legal Remedies Act, Civil Code § 1750;
e) California's Unfair Competition Law, Business and Professions Code § 17200;
f) Trespass to Personal Property / Chattels;
g) Unjust Enrichment

C. As applicable to the Classes *mutatis mutandis*, awarding injunctive and equitable relief including, *inter alia*: (i) prohibiting Clearspring and Clearspring Flash Cookie Affiliates from engaging in the acts alleged above; (ii) requiring Clearspring and Clearspring Flash Cookie Affiliates to

disgorge all of its ill-gotten gains to Plaintiffs and the other Class Members, or to whomever the Court deems appropriate; (iii) requiring Clearspring and Clearspring Flash Cookie Affiliates to delete all data surreptitiously or otherwise collected through the acts alleged above; (iv) requiring Clearspring and Clearspring Flash Cookie Affiliates to provide Plaintiffs and the other Class Members a means to easily and permanently decline any participation in any data collection activities; (v) awarding Plaintiffs and Class Members full restitution of all benefits wrongfully acquired by Clearspring and Clearspring Flash Cookie Affiliates by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Clearspring and Clearspring Flash Cookie Affiliates;

D. Award damages, including statutory damages where applicable, to Plaintiffs and Class Members in an amount to be determined at trial;

E. Award restitution against Defendants for all money to which Plaintiffs and the Classes are entitled in equity;

F. Restrain Defendants, their officers, agents, servants, employees, and attorneys, and those in active concert or participation with them from continued access, collection, and transmission of Plaintiffs and Class Members' personal information via preliminary and permanent injunction;

G. Award Plaintiffs and the Classes:

a) their reasonable litigation expenses and attorneys' fees;

b) pre- and post-judgment interest, to the extent allowable;

c) restitution, disgorgement and/or other equitable relief as the Court deems proper;

d) compensatory damages sustained by Plaintiffs and all others similarly situated as a result of Defendants' unlawful acts and conduct;

e) statutory damages, including punitive damages;

f) permanent injunction prohibiting Defendants from engaging in the conduct and practices complained of herein;

H. For such other and further relief as this Court may deem just and proper.

Dated this 9th day of August 2010

By: David Parisi

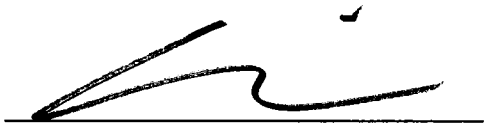
David Parisi (SBN 162248)
dcparisi@parisihavens.com
Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
Parisi & Havens LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299

Joseph H. Malley (not admitted)
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

JURY TRIAL DEMAND

The Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated this 9th day of August 2010



By: David Parisi

David Parisi (SBN 162248)
dcparisi@parisihavens.com
Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
Parisi & Havens LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299

Joseph H. Malley (not admitted)
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

DECLARATION OF DAVID C. PARISI

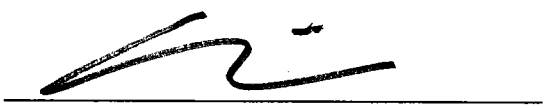
I, David C. Parisi, hereby declare on oath as follows:

1. I am an attorney licensed to practice law in the state of California. I am over the age of 18 years and I have personal knowledge of the matters attested to herein. If called upon to testify, I would and could competently do so.

2. I make this declaration pursuant to California Civil Code section 1780(c) on behalf of my clients, plaintiffs Brian White, R. H., a minor, by and through her parent, Jeff Hall, A. A., a minor, by and through her parent, Jose Aguirre, J. H., a minor, by and through his parent Jeff Hall, Kira Miles, Toni Miles, and Terrie J. Moore, on behalf of themselves and all others similarly situated.

3. Defendant Walt Disney Internet Group's principle executive offices and headquarters are located at 500 S. Buena Vista St., Burbank, CA 91521. Defendant Demand Media's principle executive offices and headquarters are located at 1333 Second Street, Santa Monica, CA 90401. Defendant Soapnet, LLC's principle executive offices and headquarters are located at 3800 W Alameda Avenue, Burbank, CA 91505. Defendant SoadHead, Inc.'s principle executive offices and headquarters are located at 15821 Ventura Blvd., Suite 260, Encino, CA 91436.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Dated this 9th day of August 2010 at Sherman Oaks, California.



David C. Parisi