



ORIGINAL

1 David Parisi (SBN 162248)
 2 dcparisi@parisihavens.com
 3 Suzanne Havens Beckman (SBN 188814)
 4 shavens@parisihavens.com
 5 Parisi & Havens LLP
 6 15233 Valleyheart Drive
 7 Sherman Oaks, California 91403
 8 Telephone: (818) 990-1299
 9
 10 Joseph H. Malley (not admitted)
 11 malleylaw@gmail.com
 12 Law Office of Joseph H. Malley
 13 1045 North Zang Blvd
 14 Dallas, TX 75208
 15 Telephone: (214) 943-6100

11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28

LODGED
 CLERK, U.S. DISTRICT COURT
 AUG 10 2010
 3:59
 CENTRAL DISTRICT OF CALIFORNIA
 DUTY
 MAD

Counsel for Plaintiffs

**IN THE UNITED STATES DISTRICT COURT
 FOR THE CENTRAL DISTRICT OF CALIFORNIA**

CV 10 5948

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. **CV 10 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;

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

4
5 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

11
12 Plaintiffs, Brian White, R. H., a minor, by and through her parent, Jeff Hall,
13 A. A., a minor, by and through her parent, Jose Aguirre, J. H., a minor, by and
14 through his parent Jeff Hall, Kira Miles, Toni Miles, and Terrie J. Moore, on behalf
15 of themselves and all others similarly situated, by and through their attorneys,
16 Parisi & Havens LLP, and Law Office of Joseph H. Malley, P.C., as and for their
17 complaint, and demanding trial by jury, allege as follows upon information and
18 belief, based upon, *inter alia*, investigation conducted by and through their
19 attorneys, which are alleged upon knowledge, sue Defendants Walt Disney Internet
20 Group, Clearspring Technologies, Inc., Demand Media, Inc., Project Playlist, Inc.,
21 Inc., Soapnet, LLC, SodaHead, Inc., Ustream, Inc., and Warner Bros. Records, Inc.
22 Plaintiffs’ allegations as to themselves and their own actions, as set forth herein are
23 based upon their personal knowledge, and all other allegations are based upon
24 information and belief pursuant to the investigations of counsel. Based upon such
25 investigation, Plaintiffs believe that substantial evidentiary support exists for the
26 allegations herein or that such allegations are likely to have evidentiary support
27 after a reasonable opportunity for further investigation and discovery.

28 **NATURE OF THE ACTION**

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

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

1 Privacy Policy, which purposes included Defendants’ commercial gain and
2 nefarious purposes.

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

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

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

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

28 7. Defendants perpetrated this exploit so they could obtain personal

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

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

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

27 URL : http://bin.clearspring.com
28 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

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

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

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

11 "Flash Cookies and Privacy," A. Soltani, S. Canty, Q. Mayo, L. Thomas, C.J.
12 Hoofnagle, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, available at
13 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 (last accessed July
14 28, 2010).

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

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

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

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

24 Flash cookies were a mistake. The company says it no longer uses
25 Flash cookies for tracking.

26 CEO Hooman Radfar says Clearspring provides software and services
27 to websites at no charge. In exchange, Clearspring collects data on
28 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:SB1000142405274870394090457539

1 [5073512989404.html](#) (last accessed August 5, 2010)

2 **JURISDICTION AND VENUE**

3
4 12. Venue is proper in this District under 28 U.S.C. §1391(b) and (c)
5 against all Clearspring Flash Cookie Affiliates. A substantial portion of the events
6 and conduct giving rise to the violations of law complained of herein occurred in
7 this District and Defendants conduct business with consumers in this District.
8 Defendant Walt Disney Internet Group's principle executive offices and
9 headquarters are located in this District at 500 S. Buena Vista St.,
10 Burbank, CA 91521. Defendant Demand Media's principle executive offices and
11 headquarters are located in this District at 1333 Second Street, Santa Monica, CA
12 90401. Defendant Soapnet, LLC's principle executive offices and headquarters are
13 located in this District at 3800 W Alameda Avenue, Burbank, CA 91505.
14 Defendant SoadHead, Inc.'s principle executive offices and headquarters are
15 located in this District at 15821 Ventura Blvd., Suite 260, Encino, CA 91436.

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

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

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

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

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

15 **PARTIES**

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

- 24 a) Warner Bros. Records

25
26 18. Plaintiff Jose Aguirre (“J. Aguirre”), is a citizen and resident of
27 Milwaukee, Wisconsin, (Milwaukee County). On information and belief, J.
28 Aguirre incorporates all allegations within this complaint. At all relevant times

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

4 a) SodaHead

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

11 a) Project Playlist, Inc.

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

18 a) SodaHead

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

25 a) Demand Media

26 22. Plaintiff Toni Miles ("T. Miles"), is a citizen and resident of Odessa,
27
28

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

6 a) SodaHead

7
8 23. Plaintiff Terrie J. Moore (“Moore”), is a citizen and resident of Grain
9 Valley, Missouri, (Jackson County). On information and belief, Moore
10 incorporates all allegations within this complaint. At all relevant times herein,
11 Moore was an Internet user that, on one or more occasions during the Class period,
12 in the city of residence, accessed online a website owned by the following named
13 Clearspring Flash Cookie Affiliate:

14 a) Soapnet

15
16 24. Plaintiff Brian White (“White”), is a citizen and resident of Diamond
17 Bar, California, (Los Angeles County). On information and belief, White
18 incorporates all allegations within this complaint. At all relevant times herein,
19 White was an Internet user that, on one or more occasions during the Class period,
20 in the city of residence, accessed online a website owned by the following named
21 Clearspring Flash Cookie Affiliate:

22 a) Ustream

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

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

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

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

10 28. Defendant Project Playlist, Inc. (hereinafter "Project Playlist"), is a
11 Delaware corporation which maintains its headquarters at 444 High Street, Suite
12 300 Palo Alto, California 94301. Defendant Project Playlist does business
13 throughout the United States, and in particular, does business in State of California
14 and in this judicial district.

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

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

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

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

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

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

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

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

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

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

- 13 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"), against
14 all Defendants;
- 15 b) California's Computer Crime Law, Penal Code § 502 (the "CCCL"),
16 against All Defendants;
- 17 c) California's Invasion Of Privacy Act, California Penal Code § 630,
18 against Clearspring;
- 19 d) California's Consumer Legal Remedies Act, Civil Code § 1750
20 ("CLRA");
- 21 e) California's Unfair Competition Law, Business and Professions Code §
22 17200 ("UCL");
- 23 f) Trespass to Personal Property / Chattels
- 24 g) Unjust Enrichment, against all Defendants.

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

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

6 **STATEMENT OF FACTS**

7 **A. Background**

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

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

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 **B. Traditional Online Advertising**

15
16 61. Commercial websites, such as Clearspring Flash Cookie Affiliates,
17 use online advertising in order to promote content to the consumers without charge
18 and require online advertising to support this objective. Commercial websites,
19 known as "publishers" allow portions of their web page to be sold to online
20 advertising networks, which act as an intermediary between "publishers" and the
21 "advertisers."

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15 **C. Web Browser Preferences**

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

22 77. Individuals have a reasonable expectation of privacy in their personal
23 computer, the integrity of their computers, and the confidentiality of their
24 communications with the Internet websites that they visit, using their Internet
25 connection to transmit and receive personal and private data, including but not
26 limited to, personal emails, personal Internet research and viewing, credit card
27 information, banking information, personal identifiable information such as social
28

1 security number, date of birth, and medical information.

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

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

20 80. Excluding the paragraph advanced by the advertising industry to
21 promulgate questionable activities to the governmental authorities and privacy
22 group, a majority of online users do not want tailored advertisements
23 Contrary to what many marketers claim, most adult Americans (66%)
24 do not want marketers to tailor advertisements to their interests.
25 Moreover, when Americans are informed of three common ways that
26 marketers gather data about people in order to tailor ads, even higher
27 percentages - between 73% and 86% - say they would not want such
28 advertising.

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

D. Flash Player- Cookies-LSO

1
2 81. Flash Player is an application that, while running on a computer that is
3 connected to the Internet, is designed to contemporaneously interact with websites
4 containing Flash content that are being visited online. As such, under certain
5 configurations, the application has the potential to silently compromise its users'
6 Internet privacy, and do so without their knowledge. When stored on a user's
7 computer, (.sol) files are capable of sending personally sensitive data back out over
8 the Internet without the user's knowledge to one or more third parties.

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

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

22 84. Functionally, client storage areas are quite different from cookies.
23 DOM Storage doesn't transmit values to the server with every request as cookies
24 do, nor does the data in a local storage area ever expire. And unlike cookies, it is
25 easy to access individual pieces of data using a standard interface that has growing
26 support among browser vendors. If objects are stored in a Local Object Repository
27 then these are available to specific actions but not to all the actions. But if these
28

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

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

12 86. Flash LSO cookies properties:

- 13 • SOL files are stored outside of the browser's cache, and removed
14 when a web browser's cache is cleared.
- 15 • By default they offer storage of 100 KB (compare: Usual cookies 4
16 KB).
- 17 • Browsers are not aware of Flash cookies, and LSO's usually cannot be
18 removed by browsers.
- 19 • Flash can access and store highly specific personal and technical
20 information (system, user name, files...).
- 21 • Ability to send the stored information to the appropriate server,
22 without user's permission.
- 23 • Flash applications do not need to be visible
- 24 • There is no easy way to tell which Flash-cookie sites are tracking you.
- 25 • Shared folders allow cross-browser tracking
- 26 • There is currently no mechanism to force a shared-object to "expire".
27 Browser cookies have an expiration mechanism built in.
- 28 • 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

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

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

15 **E. "Flash Cookies and Privacy"- Berkeley Study**

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

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

23 **F. Overlapping Values**

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

27 *It's also worth mentioning that 'tpf' and 'fpf' were found to also*
28 *contain unique identifiers which were also found to contain*

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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 users 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\F
lash
Player\#SharedObjects\3VYPOS2K\core. [name
redacted].com/#com/[name redacted]\OptOut.sol`

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

4 http://core.[name redacted].com/#com/[name redacted].
5 Retargeting.sol 3/21/2010 10:18:13 AM 5/22/2010 9:12:24 AM
6 120 C:\Users\[user's name redacted]
7 \AppData\Roaming\Macromedia\Flash
8 Player\#SharedObjects\3VYPQS2K\core. [name
9 redacted].com\#com\[name redacted].\Retargeting.sol

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

22 95. Researchers were able to indentify a high number of cookies similarly
23 labeled such as: "user ID." These cookies stored unique identifiers which allowed
24 user tracking; however unlike HTTP cookies used for tracking these cookies had
25 overlapping values. This respawning was because of the Flash cookies, provided
26 by Clearspring, had the same data values as the HTTP cookies, provided by the
27 Clearspring Flash Cookie Affiliates, so in effect the Flash cookies acted as a back-
28 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

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

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

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

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

14 **G. Defendants’ Harmful Business Practices**

15
16 98. Defendant Clearspring’s activities with Clearspring Flash Cookie
17 Affiliates occurred throughout the United States, and have secretly obtained
18 personal and private information from Plaintiffs and the Class - a course of action
19 and a body of information that is protected from interception, access, and
20 disclosure by federal law.

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

28 100. At all relevant times, Defendants’ advertising technology has

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 21 a) Loss of valuable data by attempts to remove Flash cookies once
22 discovered;
- 23 b) Incurred economic losses accompanied by an interruption in service;
- 24 c) Functionality of computer interfered with, including an inability of
25 websites visited once Flash content was disabled;
- 26 d) Information was deleted, otherwise made unavailable;
- 27 e) Impaired the integrity and availability of data, programs and
28 information.

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

9 **CLASS ALLEGATIONS**
10 **Allegations as to Class Certification**

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

- 15 a) U.S. Resident Class: All persons residing in the United States that
16 accessed a Clearspring Flash Cookie Affiliate website and a Flash
17 cookie was set on their computer to use its local storage within the
18 Flash media player to back up browser cookies for the purposes of
19 restoring them later.
- 20 b) California Resident Class: All persons residing in California that
21 accessed a Clearspring Flash Cookie Affiliate website and a Flash
22 cookie was set on their computer to use its local storage within the
23 Flash media player to back up browser cookies for the purposes of
24 restoring them later. All California Resident Class Members are also
25 members of the U.S. Resident Class.
- 26 c) Injunctive Class: All persons after the date of the filing of this
27 complaint, residing in the United States, that accessed a Clearspring
28 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

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

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

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

- 10 a) Computer Fraud and Abuse Act ("CFAA"),
- 11 b) California's Computer Crime Law, ("CCCL"),
- 12 c) Trespass to Personal Property / Chattels, and
- 13 d) Unjust Enrichment against *ALL DEFENDANTS*:
14 All persons residing in United States who, during the period of
15 two years preceding the date of this filing to the date of Class
16 certification (the "Class Period"), accessed a Clearspring Flash
17 Cookie Affiliate website and a Flash cookie was set on their
18 computer to use its local storage within the Flash media player
19 to back up browser cookies for the purposes of restoring them
20 later.
21 (hereinafter referred to as "CFAA/ ECPA/CCCL SubClass.")

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

- 25 a) California's Computer Crime Law ("CCCL"),
- 26 b) California's Invasion of Privacy Act, against *DEFENDANT*
27 *CLEARSPRING, ALONE*:
28 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.")

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

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

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

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

- 16 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
17 b) California's Computer Crime Law, Penal Code § 502;
18 c) California Invasion Of Privacy Act, California Penal Code § 630;
19 d) Trespass to Personal Property / Chattels;
20 e) Unjust Enrichment

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

23 136. **Persons Excluded From Classes:** Subject to additional information
24 obtained through further investigation and discovery, the foregoing definition of
25 the Class may be expanded or narrowed by amendment or amended complaint.
26 Specifically excluded from the proposed Class are Defendants, their officers,
27 directors, agents, trustees, parents, children, corporations, trusts, representatives,
28 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

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

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

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

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

- 18 a) What was the extent of Clearspring and Clearspring Flash Cookie
19 Affiliates' business practice of setting a Flash cookie on a user's
20 computer to use its local storage within the Flash media player to
21 back up browser cookies for the purpose of restoring them later
22 and how did it work?
- 23 b) What information did Clearspring and Clearspring Flash Cookie
24 Affiliates' collect from its business practices of setting a Flash
25 cookie on a user's computer to use its local storage within the
26 Flash media player to back up browser cookies for the purpose of
27 restoring them later, and what did it do with that information?
- 28 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

1 practices of setting a Flash cookie on a user's computer to use its
2 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?

- 3 e) Was there reasonable opportunity to decline the operation of
4 Clearspring and Clearspring Flash Cookie Affiliates' business
practices of setting a Flash cookie on a user's computer to use its
5 local storage within the Flash media player to back up browser
cookies for the purpose of restoring them later provided to
6 Clearspring and Clearspring Flash Cookie Affiliates' users?
- 7 f) Did Clearspring and Clearspring Flash Cookie Affiliates' business
practices of setting a Flash cookie on a user's computer to use its
8 local storage within the Flash media player to back up browser
cookies for the purpose of restoring them later disclose, intercept,
9 and transmit personally identifying information, or sensitive
identifying information, or personal information?
- 10 g) Whether Clearspring and Clearspring Flash Cookie Affiliates
11 devised and deployed a scheme or artifice to defraud or conceal
from Plaintiffs and the Class Clearspring and Clearspring Flash
12 Cookie Affiliates' ability to, and practice of, intercepting,
accessing, and manipulating, for its own benefit, personal
13 information, and tracking data from Plaintiffs' and the Class'
personal computers via the ability to; (and practice of) implanting
14 secret "cookies" on their computers;
- 15 h) Whether Clearspring and Clearspring Flash Cookie Affiliates
engaged in deceptive acts and practices in, connection with its
16 undisclosed and systemic practice of implanting, accessing and/or
disclosing unique identifiers, tracking data, and personal
17 information on Plaintiffs and the Class' personal computers and
using that data to track and profile Plaintiffs' and the Class'
18 Internet activities and personal habits, proclivities, tendencies, and
preferences for defendants' use and benefit;
- 19 i) Did the implementation of Clearspring and Clearspring Flash
20 Cookie Affiliates' business practices of setting a Flash cookie on a
user's computer to use its local storage within the Flash media
21 player to back up browser cookies for the purpose of restoring
them later violate the Computer Fraud and Abuse Act, 18 U.S.C.
22 §§ 1030?
- 23 j) Did the operation, function, and/or implementation of Clearspring
and Clearspring Flash Cookie Affiliates' business practices of
24 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
25 purpose of restoring them later violate California's Computer
Crime Law, California Penal Code § 502?
- 26 k) Did the operation, function, and/or implementation of Clearspring
and Clearspring Flash Cookie Affiliates' business practices of
27 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
28 purpose of restoring them later violate the California Invasion of

Privacy Act, California Penal Code § 630?

- 1
 - 2
 - 3
 - 4
 - 5
 - 6
 - 7
 - 8
 - 9
 - 10
 - 11
 - 12
 - 13
 - 14
 - 15
 - 16
 - 17
 - 18
 - 19
 - 20
 - 21
 - 22
 - 23
 - 24
 - 25
 - 26
 - 27
 - 28
- 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

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

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

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

- 19
- 20 a) the prosecution of separate actions by individual Class Members
21 would create a risk of inconsistent or varying adjudication with
22 respect to individual Class Members that would establish
23 incompatible standards of conduct for the Defendants;
 - 24 b) the prosecution of separate actions by individual Class Members
25 would create a risk of adjudications with respect to them that
26 would, as a practical matter, be dispositive of the interests of other
27 Class Members not parties to the adjudications, or substantially
28 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.

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

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

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

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

13 **Count I**
14 **Violation of the Computer Fraud and Abuse Act**
15 **18 U.S.C. § 1030 *et seq.***
16 **Against All Defendants**

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

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

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

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

1 obtaining information from such a protected computer.

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

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

10 154. Plaintiffs’ computer is a “protected computer...which is used in
11 interstate commerce and/or communication” within the meaning of 18 U.S.C. §
12 1030(e)(2)(B).

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

16 156. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly
17 causing the transmission of a command embedded within their webpages,
18 downloaded to Plaintiffs’ computer, which are protected computers as defined in
19 18 U.S.C. § 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs’
20 viewing habits, Defendants intentionally caused damage without authorization to
21 those Plaintiffs’ computers by impairing the integrity of the computer.

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

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

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

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

6 160. Plaintiffs have suffered loss by reason of these violations, as defined
7 in 18 U.S.C. § 1030(e)(11), by the “reasonable cost ... including the cost of
8 responding to an offense, conducting a damage assessment, and restoring the data,
9 program, system, or information to its condition prior to the offense, and any
10 revenue lost, cost incurred, or other consequential damages incurred because of
11 interruption of service.”

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

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

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

23 164. Defendants’ unlawful access to Plaintiffs’ computers and electronic
24 communications has caused Plaintiffs irreparable injury. Unless restrained and
25 enjoined, Defendants will continue to commit such acts. Plaintiffs’ remedy at law
26 is not adequate to compensate it for these inflicted and threatened injuries, entitling
27 Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C. §
28 1030(g).

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

1 legitimate users of a computer system, network, or program.”

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

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

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

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

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

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

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

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

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

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

13 181. California Penal Code § 502(j) states: "For purposes of bringing a
14 civil or a criminal action under this section, a person who causes, by any means,
15 the access of a computer, computer system, or computer network in one
16 jurisdiction from another jurisdiction is deemed to have personally accessed the
17 computer, computer system, or computer network in each jurisdiction."

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

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

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

1 to Plaintiffs in an amount to be proven at trial. Plaintiffs are also entitled to
2 recover their reasonable attorneys' fees pursuant to California Penal Code §
3 502(e).

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

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

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

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

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

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

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

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

2
3 Any person who, . . . or who willfully and without the consent of all
4 parties to the communication, or in any unauthorized manner, reads,
5 or attempts to read, or to learn the contents or meaning of any
6 message, report, or communication while the same is in transit or
7 passing over any wire, line, or cable, or is being sent from, or received
8 at any place within this state; or who uses, or attempts to use, in any
9 manner, or for any purpose, or to communicate in any way, any
10 information so obtained, or who aids, agrees with, employs, or
11 conspires with any person or persons to unlawfully do, or permit, or
12 cause to be done any of the acts or things mentioned above in this
13 section, is punishable . . .

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

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

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

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

27 196. Defendants are not a "public utility engaged in the business of
28 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

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

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

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

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

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

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

21 **COUNT IV**
22 **Violations of the Consumer Legal Remedies Act**
23 **(“CLRA”) California Civil Code § 1750, et seq.**
24 **Against All Defendants**

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

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

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

- 6
- 7 a) Defendants’ representations that their services have
 - 8 characteristics, uses, and benefits that they do not have, in
 - 9 violation of Civil Code § 1770(a)(5);
 - 10 b) Defendants’ representations that their services are of a particular
 - 11 standard, quality and grade but are of another standard quality and
 - 12 grade, in violation of Civil Codes § 1770(a)(7); and
 - 13 c) Defendants’ advertisement of services with the intent not to sell
 - 14 those services as advertised, in violation of Civil Code §
 - 15 1770(a)(9).

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

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

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

28

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

1
2
3
4 209. Plaintiffs incorporate the foregoing allegations as if fully set forth
5 herein.

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

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

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

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

26 214. Defendants’ business acts and practices are unfair because they cause
27 harm and injury-in-fact to Plaintiffs and Class Members and for which Defendants
28

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

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

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

22 **Count VI**
23 **Trespass to Personal Property / Chattels**
24 **Against All Defendants**

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

27 218. The common law prohibits the intentional intermeddling with
28 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,

1 quality, or usefulness of the personal property.

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

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

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

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

- 19 a) Defendants accessed and obtained control over the user's
20 computer;
- 21 b) Defendants caused the installation of a new code onto the hard
22 drive of the user's computer;
- 23 c) Defendants programmed the operation of its code to function and
24 operate without notice or consent on the part of the owner of the
25 computer, and outside of the control of the owner of the computer.

26
27 223. All these acts described above were acts in excess of any authority
28 any user granted when he or she visited the Clearspring Flash Cookie Affiliates'

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

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

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

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

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

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

- 20 a) By consuming the resources of and/or degrading the performance
21 of Plaintiffs' and Class Members' computers (including hard drive
22 space, memory, processing cycles, and Internet connectivity);
23 b) By diminishing the use of, value, speed, capacity, and/or
24 capabilities of Plaintiffs' and Class Members' computers;
25 c) By devaluing, interfering with, and/or diminishing Plaintiffs' and
26 Class Members' possessory interest in their computers;
27 d) By altering and controlling the functioning of Plaintiffs' and Class
28 Members' computers;

- 1 e) By infringing on Plaintiffs' and Class Members' right to exclude
- 2 others from their computers;
- 3 f) By infringing on Plaintiffs' and Class Members' right to
- 4 determine, as owners of their computers, which programs should
- 5 be installed and operating on their computers;
- 6 g) By compromising the integrity, security, and ownership of Class
- 7 Members' computers; and
- 8 h) By forcing Plaintiffs and Class Members' to expend money, time,
- 9 and resources in order to remove the program installed on their
- 10 computers without notice or consent.

11 **Count VII**
12 **Unjust Enrichment**
13 **Against All Defendants**

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

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

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

25 232. Defendants appreciate or have knowledge of said benefit.

26 233. Under principles of equity and good conscience, Defendants should
27 not be permitted to retain the information and/or revenue which they acquired by
28

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

4
5 **PRAYER FOR RELIEF**

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

8
9 A. Certify this case as a Class action on behalf of the Classes defined above,
10 appoint Plaintiffs as Class representatives, and appoint their counsel as Class
11 counsel;

12
13 B. Declare that the actions of Clearspring and Clearspring Flash Cookie
14 Affiliates, as set out above, violate the following:

- 15 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- 16 b) California's Computer Crime Law, Penal Code § 502;
- 17 c) California's Invasion Of Privacy Act, California Penal Code § 630;
- 18 d) California's Consumer Legal Remedies Act, Civil Code § 1750;
- 19 e) California's Unfair Competition Law, Business and Professions Code
20 § 17200;
- 21 f) Trespass to Personal Property / Chattels;
- 22 g) Unjust Enrichment

23
24 C. As applicable to the Classes *mutatis mutandis*, awarding injunctive and
25 equitable relief including, *inter alia*: (i) prohibiting Clearspring and
26 Clearspring Flash Cookie Affiliates from engaging in the acts alleged above;
27 (ii) requiring Clearspring and Clearspring Flash Cookie Affiliates to
28

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

15
16 D. Award damages, including statutory damages where applicable, to Plaintiffs
17 and Class Members in an amount to be determined at trial;

18
19 E. Award restitution against Defendants for all money to which Plaintiffs and
20 the Classes are entitled in equity;

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

25
26 G. Award Plaintiffs and the Classes:

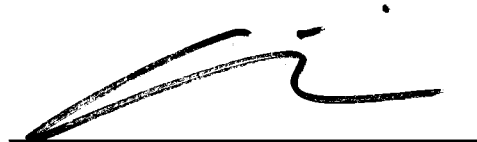
27 a) their reasonable litigation expenses and attorneys' fees;

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

- 1 c) restitution, disgorgement and/or other equitable relief as the Court
- 2 deems proper;
- 3 d) compensatory damages sustained by Plaintiffs and all others similarly
- 4 situated as a result of Defendants' unlawful acts and conduct;
- 5 e) statutory damages, including punitive damages;
- 6 f) permanent injunction prohibiting Defendants from engaging in the
- 7 conduct and practices complained of herein;

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

9
10 Dated this 9th day of August 2010

11 
12 _____
13 By: David Parisi

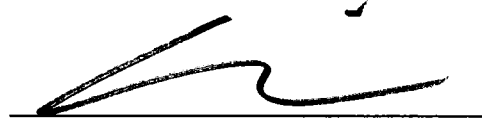
14 David Parisi (SBN 162248)
15 dcparisi@parisihavens.com
16 Suzanne Havens Beckman (SBN 188814)
17 shavens@parisihavens.com
18 Parisi & Havens LLP
19 15233 Valleyheart Drive
20 Sherman Oaks, California 91403
21 Telephone: (818) 990-1299

22 Joseph H. Malley (not admitted)
23 malleylaw@gmail.com
24 Law Office of Joseph H. Malley
25 1045 North Zang Blvd
26 Dallas, TX 75208
27 Telephone: (214) 943-6100
28

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DECLARATION OF DAVID C. PARISI

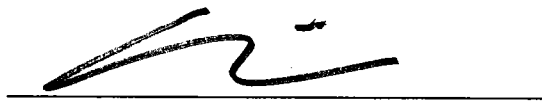
I, David C. Parisi, hereby declare on oath as follows:

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