

1 David Parisi (SBN 162248)  
2 [dcparsi@parisihavens.com](mailto:dcparsi@parisihavens.com)  
3 Parisi & Havens LLP  
4 15233 Valleyheart Drive  
5 Sherman Oaks, California 91403  
6 Telephone: (818) 990-1299

7 Joseph H. Malley (not admitted)  
8 malleylaw@gmail.com  
9 Law Office of Joseph H. Malley  
10 1045 North Zang Blvd  
11 Dallas, TX 75208  
12 Telephone: (214) 943-6100

13 *Counsel for Plaintiffs*

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

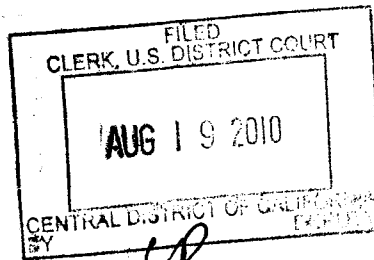
16 GENEVIVE LA COURT; DEIRDRE  
17 HARRIS; CAHILL HOOKER; BILL  
18 LATHROP; JUDY STOUGH; and E.H., a  
19 minor, by and through her parent, JEFF  
20 HALL; individuals, on behalf of themselves  
21 and others similarly situated,

22 Plaintiffs,

23 v.

24 SPECIFIC MEDIA, INC., a Delaware  
25 Corporation;

26 Defendants.



BY:

A handwritten signature, possibly 'CP', written in black ink.

CLERK U.S. DISTRICT COURT  
CENTRAL DIST. OF CALIF.  
LOS ANGELES

10 AUG 18 PM 12:14

LOGGED

14 SACV10-01256 JVS  
15 CASE No. VBKX

16 JURY DEMAND

17 CLASS ACTION  
18 COMPLAINT FOR:

- 19 1. Violation of Computer  
20 Fraud and Abuse Act, 18  
21 U.S.C. § 1030;
- 22 2. Violation of California's  
23 Computer Crime Law,  
24 Penal Code § 502;
- 25 3. Violation of California's  
26 Invasion Of Privacy Act,  
27 California Penal Code §  
28 630;
4. Violation of California's

IIS  
21  
4/N

Class Action Complaint

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

Consumer Legal Remedies Act, Civil Code § 1750;

5. Violation of California's Unfair Competition Law, Business and Professions Code § 17200;

6. Trespass to Personal Property / Chattels

7. Unjust Enrichment

Plaintiffs Genevieve La Court, Deirdre Harris, Cahill Hooker, Bill Lathrop, Judy Stough, and E.H., a minor, by and through her parent, Jeff Hall, on behalf of themselves and all others similarly situated, by and through their attorneys, Parisi & Havens LLP, and Law Office of Joseph H. Malley, P.C., as and for their complaint, and demanding trial by jury, allege as follows upon information and belief, based upon, *inter alia*, investigation conducted by and through their attorneys, which are alleged upon knowledge, sue Defendant Specific Media, Inc., Plaintiffs' allegations as to themselves and their own actions, as set forth herein are based upon their personal knowledge, and all other allegations are based upon information and belief pursuant to the investigations of counsel. Based upon such investigation, Plaintiffs believe that substantial evidentiary support exists for the allegations herein or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and discovery.

**NATURE OF THE ACTION**

1. Plaintiffs bring this consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of themselves and a class of similarly situated Internet users, each a "Class Member"

1 of the putative “Class,” as further described herein, who were victims of fraud and  
2 unfair business practices; wherein their privacy, financial interests, and computer  
3 security rights, were violated by the following Defendant (“Defendant”): Specific  
4 Media, Inc., (hereinafter referred to as “Specific Media”), in concert with websites,  
5 and its “counter and statistics” tracking services affiliated individually with  
6 Specific Media, referred collectively to as, “SpecificClick Flash Cookie  
7 Affiliates,” by setting Flash cookies on their users’ computers to use the Flash  
8 Media Player local storage Flash on those computers to back up browser cookies  
9 for the purposes of restoring them later.

10         2.       SpecificClick Flash Cookie Affiliates each independently, with  
11 Specific Media, knowingly authorized, directed, ratified, approved, acquiesced in,  
12 or participated in conduct made the basis of this Class action, which included, but  
13 was not limited to, setting of an online tracking device which would allow access  
14 to and disclosure of Internet users’ online activities as well as personal information  
15 (“PI”), personal identifying information (“PII”), and/or sensitive indentifying  
16 information (“SII”) derived from such online activities, including but not limited  
17 to, users’ activities on non-SpecificClick Flash Cookie Affiliates’ websites, and its  
18 tracking services, and which Defendant accomplished covertly, without actual  
19 notice to users, awareness by users, or consent and choice of users, and which  
20 information Defendant obtained deceptively, for purposes not disclosed within  
21 their Terms of Service and/or Privacy Policy, which purposes included  
22 Defendant’s commercial gain and nefarious purposes.

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

28         4.       SpecificClick Flash Cookie Affiliates are websites, and tracking

1 services, which acted with Defendant Specific Media, independently of one  
2 another, and hacked the computers of millions of consumers' computers to plant  
3 rogue, cookie-like tracking code on users' computers. With this tracking code,  
4 Defendant circumvented users' browser controls for managing web privacy and  
5 security.

6         5. Plaintiffs and Class Members that visited the websites of the  
7 SpecificClick Flash Cookie Affiliates had tracking codes installed on their  
8 computers by Defendant Specific Media acting in concert with the respective  
9 SpecificClick Flash Cookie Affiliate website, and/ or in concert with its  
10 SpecificClick Flash Cookie Affiliate website tracking service, without notice or  
11 consent, and which tracking codes could not easily be detected, managed or  
12 deleted. In cooperation with the SpecificClick Flash Cookie Affiliates, Specific  
13 Media planted its own tracking code on users' computers—but not in a browser  
14 cookie. Specific Media and SpecificClick Flash Cookie Affiliates stored tracking  
15 code as Adobe Flash Media Player local shared objects (LSOs). Adobe Flash  
16 Media Player is software that enables users to view video content on their  
17 computers.

18         6. Once the tracking code was installed by the Defendant, such provided  
19 the mechanism to track Plaintiffs and Class Members that visited non-  
20 SpecificClick Flash Cookie Affiliates websites by having their online  
21 transmissions intercepted, without notice or consent; moreover if the user deleted  
22 the browser cookie, the Flash cookie would be used to “re-spawn” the browser  
23 cookie.

24         7. Defendant perpetrated this exploit so they could obtain personal  
25 identifying information, monitor users, and to sell users' data. The personal  
26 information Defendant misappropriated and compiled, with information provided  
27 from Specific Media and SpecificClick Flash Cookie Affiliates includes details  
28 about user profiles to identify individual users and track them on an ongoing basis,

1 across numerous websites, even spotting and tracking users when they accessed the  
2 web from different computers, at home and at work. This sensitive information  
3 may include such things as users' video viewing choices and personal  
4 characteristics such as gender, age, race, number of children, education level,  
5 geographic location, and household income, what the web user looked at and what  
6 he/she bought, the materials he/she read, details about his/her financial situation,  
7 his/her sexual preference, his/her name, home address, e-mail address and  
8 telephone number, and even more specific information like health conditions, such  
9 as DEPRESSION.

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

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

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

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

1 “Flash Cookies and Privacy,” A. Soltani, S. Canty, Q. Mayo, L. Thomas, C.J.  
2 Hoofnagle, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, available at  
3 [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1446862](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862) (last accessed July  
4 28, 2010).

5 10. Defendant’s use of the Adobe Flash Media Player for tracking online  
6 users was condemned by Adobe:

7 *“Adobe condemns the practice of using Local Storage to back up  
8 browser cookies for the purpose of restoring them later without user  
9 knowledge and express consent.”*

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

12 *“A few months back, StatCounter was approached by an advertiser,  
13 offered lots of \$\$\$, and asked to include a spyware cookie on all of  
14 our member sites...we refused on the spot.*

15 *You install StatCounter to track visitors to your site NOT to open  
16 yourself and your visitors up to being spied upon by phantom  
17 advertising corporations.*

18 *It appears, however, that other players in the world of webstats were  
19 happy to take up this offer...*

20 *We were shocked to discover just today that another well known stats  
21 provider is allowing up to 9 cookies to be installed in the browser of  
22 every visitor that hits one of their member websites. This means that  
23 the provider is making money by transmitting data on you and your  
24 visitors to a third party advertiser. Not only that, but to add insult to  
25 injury, the cookies are causing the member websites to load very  
26 slowly too.”*

27 <http://blog.statcounter.com/2007/03/statcounter-says-no/> (last accessed August 12,  
28 2010)

*“SiteMeter, a well-known web stats providers, is pushing specificclick  
tracking and advertising cookies on to visitors of sites using their  
service.”*

3 **JURISDICTION AND VENUE**

4 11. Venue is proper in this District under 28 U.S.C. §1391(b) and (c)  
5 against Defendant. A substantial portion of the events and conduct giving rise to  
6 the violations of law complained of herein occurred in this District and Defendant  
7 conducts business with consumers in this District. Defendant Specific Media's  
8 principle executive offices and headquarters are located in this District at 4 Park  
9 Plaza, Suite 1500, Irvine, California 92614.

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

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

25 14. Minimal diversity of citizenship exists in this action, providing  
26 jurisdiction as proper in the Court, since Defendant is a corporation headquartered  
27 in this District, and Plaintiffs include citizens and residents of this District, and  
28

1 assert claims on behalf of a proposed Class whose members are scattered  
2 throughout the fifty states and the U.S. territories; thus there is minimal diversity of  
3 citizenship between proposed Class Members and the Defendant.

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

### 9 **PARTIES**

10 16. Plaintiff Genevieve La Court (“G. La Court”), is a citizen and resident  
11 of Los Angeles, California, (Los Angeles County). On information and belief, G.  
12 La Court incorporates all allegations within this complaint. G. La Court is a  
13 representative of the “U.S. Resident Class,” the “California Class,” and the  
14 “Injunctive Class” defined within the Class Allegations. At all relevant times  
15 herein, G. La Court experience(s) related to the Defendant was as an Internet user  
16 that, on one or more occasions during the Class period, in the city of residence,  
17 accessed online a website owned and operated by a SpecificClick Flash Cookie  
18 Affiliate, which included a SpecificClick Flash Cookie Affiliate website tracking  
19 service, and had a Defendant Flash Cookie tracking device embedded within their  
20 computer.

21 17. Plaintiff Deirdre Harris (“D. Harris”), is a citizen and resident of  
22 Andrews, Texas, (Andrews County). On information and belief, D. Harris  
23 incorporates all allegations within this complaint. D. Harris is a representative of  
24 the “U.S. Resident Class” and the “Injunctive Class” defined within the Class  
25 Allegations. At all relevant times herein, D. Harris experience(s) related to the  
26 Defendant was as an Internet user that, on one or more occasions during the Class  
27 period, in the city of residence, accessed online a website owned and operated by a  
28



1 SpecificClick Flash Cookie Affiliate, which included a SpecificClick Flash Cookie  
2 Affiliate website tracking service, and had a Defendant Flash Cookie tracking  
3 device embedded within their computer.

4 18. Plaintiff Cahill Hooker (“C. Hooker”), is a citizen and resident of  
5 Dallas, Texas, (Dallas County). C. Hooker is a representative of the “U.S.  
6 Resident Class” and the “Injunctive Class” defined within the Class Allegations.  
7 On information and belief, C. Hooker incorporates all allegations within this  
8 complaint. At all relevant times herein, C. Hooker experience(s) related to the  
9 Defendant was as an Internet user that, on one or more occasions during the Class  
10 period, in the city of residence, accessed online a website owned and operated by a  
11 SpecificClick Flash Cookie Affiliate, which included a SpecificClick Flash Cookie  
12 Affiliate website tracking service, and had a Defendant Flash Cookie tracking  
13 device embedded within their computer.

14 19. Plaintiff Bill Lathrop (“B. Lathrop”), is a citizen and resident of  
15 Pahrump, Nevada, (Nye County). On information and belief, B. Lathrop  
16 incorporates all allegations within this complaint. B. Lathrop is a representative of  
17 the “U.S. Resident Class” and the “Injunctive Class” defined within the Class  
18 Allegations. At all relevant times herein, B. Lathrop experience(s) related to the  
19 Defendant was as an Internet user that, on one or more occasions during the Class  
20 period, in the city of residence, accessed online a website owned and operated by a  
21 SpecificClick Flash Cookie Affiliate, which included a SpecificClick Flash Cookie  
22 Affiliate website tracking service, and had a Defendant Flash Cookie tracking  
23 device embedded within their computer.

24 20. Plaintiff Judy Stough (“J. Stough”), is a citizen and resident of  
25 Garland, Texas, (Dallas County). On information and belief, J. Stough incorporates  
26 all allegations within this complaint. J. Stough is a representative of the “U.S.  
27 Resident Class” and the “Injunctive Class” defined within the Class Allegations.  
28 At all relevant times herein, J. Stough experience(s) related to the Defendant was

1 as an Internet user that, on one or more occasions during the Class period, in the  
2 city of residence, accessed online a website owned and operated by a SpecificClick  
3 Flash Cookie Affiliate, which included a SpecificClick Flash Cookie Affiliate  
4 website tracking service, and had a Defendant Flash Cookie tracking device  
5 embedded within their computer.

6 21. Plaintiff E.H. (“E. H.”), is a citizen and resident of Forney, Texas,  
7 (Kaufman County), and a minor, represented by and through her parent Jeff Hall.  
8 On information and belief, E. H. incorporates all allegations within this complaint.  
9 E.H. is a representative of the “U.S. Resident Class” and the “Injunctive Class”  
10 defined within the Class Allegations. At all relevant times herein, E. H.  
11 experience(s) related to the Defendant was as an Internet user that, on one or more  
12 occasions during the Class period, in the city of residence, accessed online a  
13 website owned and operated by a SpecificClick Flash Cookie Affiliate, which  
14 included a SpecificClick Flash Cookie Affiliate website tracking service, and had a  
15 Defendant Flash Cookie tracking device embedded within their computer.

16 22. Defendant Specific Media, Inc., doing business online, using domains  
17 which include, but not limited to: SpecificClick, Specificclick.net, and  
18 Specificclick.com (hereinafter referred to as “Specific Media”), is a Delaware  
19 corporation which maintains its headquarters at 4 Park Plaza, Suite 1500, Irvine,  
20 California 92614. Defendant Specific Media, Inc., does business throughout the  
21 United States, and in particular, does business in State of California and in this  
22 County.

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

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

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

16           26. The conduct complained of includes, but not limited to, the  
17 interception of electronic communication of Plaintiffs and Class Members  
18 involving non-SpecificClick Flash Cookie Affiliates, obtained in transit and  
19 temporarily stored for a limited period in their computer's electronic storage. *In re:*  
20 *DoubleClick, Inc. Privacy Litigation*, 154 F. Supp.2d 497,00 Civ. 0641 (S.D.N.Y.,  
21 March 28, 2001)

22           27. The conduct of Specific Media individually and in concert with the  
23 SpecificClick Flash Cookie Affiliates, individually and jointly, is a fraud that has  
24 been perpetrated for years, facilitated, and coordinated, by some of the world's  
25 largest websites and the network advertising industry, thereby costing the Class  
26 upwards of tens of millions of dollars. Defendant has been systematically  
27 defrauding Class Members in a covert operation of surveillance made possible by  
28 their gross misconduct, negligence, apparent coordination, and actual fraud, and

1 violating one (1) or more of the following:

- 2 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the “CFAA”);
- 3 b) California’s Computer Crime Law, Penal Code § 502 (the “CCCL”);
- 4 c) California’s Invasion Of Privacy Act, California Penal Code § 630;
- 5 d) California’s Consumer Legal Remedies Act, Civil Code § 1750  
6 (“CLRA”);
- 7 e) California’s Unfair Competition Law, Business and Professions Code §  
8 17200 (“UCL”);
- 9 f) Trespass to Personal Property / Chattels; and
- g) Unjust Enrichment

10 28. SpecificClick Flash Cookie Affiliates’ privacy documents omit  
11 entirely the actual identity of its association with Specific Media, limiting the  
12 user’s awareness of, and an inability to determine accurately, the involvement of  
13 Specific Media, or locate the Specific Media website, compounded further by  
14 Specific Media defining its business as a media measurement and web analytics  
15 company while the SpecificClick Flash Cookie Affiliates’ privacy documents refer  
16 only to associations involving advertising networks.

17 29. Defendant Specific Media and SpecificClick Flash Cookie Affiliates’  
18 privacy documents describe “associations,” misleading the users which interpret  
19 such to be associated corporate subsidiaries, withholding accurate information that  
20 such includes other entities than advertising networks, such as: data exchanges,  
21 traffic measurement service providers, and marketing analytics service providers.

22 30. Defendant Specific Media and SpecificClick Flash Cookie Affiliates’  
23 websites, and its tracking services, are owned by parent companies that have many  
24 subsidiaries and fail to provide adequate information about third-party information  
25 sharing, different than affiliate sharing, which is subject to more restrictions,  
26 including opt-in or opt-out consent requirements. These restrictions are based upon  
27 the heightened risk associated with sharing information with unrelated entities,  
28 which have different incentives than the entity that collected the user data.

1           31. Defendant Specific Media and SpecificClick Flash Cookie Affiliates  
2 do not make adequate distinctions between sharing with affiliates, contractors, and  
3 third parties, instead, vaguely stating that they do not share user data with unrelated  
4 third parties and vaguely disclosing that they share data with affiliates. Users must  
5 interpret an affiliate to be a third party, but given the actual usage of these terms of  
6 SpecificClick Flash Cookie Affiliates' privacy policies, that assumption would be  
7 mistaken.

8           32. Defendant Specific Media and SpecificClick Flash Cookie Affiliate  
9 users are unable to identify the corporate families to which these Defendant  
10 websites belong; which makes it difficult for a user to discover exactly who such  
11 associated entities are, thus their practices are deceptive. A practice is deceptive if  
12 it involves a representation, omission or practice that is likely to mislead a  
13 consumer acting reasonably in the circumstances, to the consumer's detriment. The  
14 conflicting statements in the privacy policies would most likely confuse or mislead  
15 a reasonable consumer. The confusion would also likely be to their detriment, as  
16 surveys indicate that users do not want companies to collect data about them  
17 without permission.

18           33. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
19 privacy documents discuss that the data collection practices of entities associated  
20 with their corporations are outside the coverage of their privacy policies. This  
21 appears to be an attempt to create a critical loophole used by SpecificClick Flash  
22 Cookie Affiliates compounding their attempts to violate the privacy protection of  
23 their users.

24           34. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
25 privacy documents fail to provide adequate notice that Defendant Specific Media  
26 and SpecificClick Flash Cookie Affiliates allow access to personal behavioral data  
27 of their users, including but not limited to, such data embedded with their cookies,  
28 to Specific Media, which in turn shares the data with its marketing partners or

1 corporate affiliates and subsidiaries, meaning that user behavior will be profiled by  
2 any other entities with whom those sites may choose to share this information.

3 Defendant Specific Media and SpecificClick Flash Cookie Affiliates state they do  
4 not share data with third parties, but they do share data with affiliates, suggesting  
5 that they only share data with companies under the same corporate ownership.

6 35. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
7 privacy documents referenced the use of Flash cookies, but state such is used only  
8 for audience measurement and not behavioral ad-targeting. The opt-out is  
9 inconspicuous on their privacy page and appears in a small font header in the  
10 corner of the page.

11 36. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
12 privacy documents do not expressly state that if a SpecificClick Flash Cookie  
13 Affiliate user opts out that behavioral information will not be collected and shared,  
14 but only that the Defendant Specific Media and SpecificClick Flash Cookie  
15 Affiliate user will not receive Internet based advertising content from its  
16 "advertising delivery service"; moreover its opt-out "unique cookie value" includes  
17 identifying information which means the cookie is no longer non-unique.

18 37. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
19 privacy documents falsely imply some level of protection for the user. Defendant  
20 Specific Media and SpecificClick Flash Cookie Affiliates' privacy documents are  
21 sufficiently vague so as to refrain from fully disclosing information to their users  
22 about what information is collected through their websites and their associated  
23 entities, how the information is used, and the purposes for the collection and use of  
24 this information, negating the possibility for their users to provide informed and  
25 meaningful consent to these practices. Without adequate notice and informed and  
26 meaningful user consent, users had no control over their personal information,  
27 thus, the potential privacy dangers were not readily apparent to most users.

28 38. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'

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

4 39. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
5 privacy documents incorporate a multitude of hedging and modality markers so as  
6 to minimize their use of covert surveillance technology and data-gathering tools,  
7 while sending mixed messages related to privacy controls, advising users that  
8 choosing to exercise such controls would cause in whole, or part, diminished  
9 functionality of their websites, while such documents emphasize all cookies are  
10 very small, thus unobtrusive, and pose no threat since "many websites use them."

11 40. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
12 privacy documents fail to adhere to an adequate notice and choice regime,  
13 predicated on user choice, and informed by privacy policies. Defendant Specific  
14 Media and SpecificClick Flash Cookie Affiliates' privacy documents provided  
15 nuanced situations that created conditional yes or no answers to these basic  
16 questions about a site's data collection and sharing practices, thus it is unclear how  
17 an average user could ever understand these practices since the nuances were not  
18 explained in the privacy policy. Choice, therefore, cannot be inferred.

19 41. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
20 privacy documents fail to provide notice that their data storage practices as they  
21 relate to the period for which user data is stored, have no term period and are  
22 indefinite.

23 42. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
24 privacy documents carefully attempt to parse the definitions of phrases related to  
25 their tracking activity. Their privacy documents are more nuanced than such  
26 categorized analysis allows for, omitting any direct reference to Flash cookies,  
27 embedding surveillance technology into the user's computer hardware, use of  
28 user's computer hardware to store data, use of technology to allow the perpetual

1 online tracking and surveillance of any and all online Internet activity of the  
2 SpecificClick Flash Cookie Affiliate user. They also refrain from disclosing that  
3 the SpecificClick Flash Cookie Affiliate would use the user's local storage to back  
4 up browser cookies for the purpose of restoring them later without user knowledge  
5 and express consent, as evidenced by the attempt to hide its covert activity by  
6 referring to their use of "other technologies," or "similar technologies" to cookies  
7 and web beacons, in lieu of Flash cookies which would have perpetual existence  
8 on a user's computer and the ability to respawn, i.e. "zombie cookies."

9 43. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
10 privacy documents' verbiage was deceptive by design. This deception is especially  
11 troubling when compared with the obligation imposed upon their online visitors to  
12 download, read, and comprehend the vast amount of documents required to protect  
13 one's online privacy, complicated by the cumulative effect of such task.

14 44. In addition to downloading, reading and comprehending all of the  
15 SpecificClick Flash Cookie Affiliates websites privacy documents, its users would  
16 be required to locate and do the same for the website for the SpecificClick Flash  
17 Cookie Affiliates "counter and statistic tracker" entity, then locate and do the same  
18 for Specific Media and repeat this obligation. To accentuate the improbability of  
19 completing this task though, SpecificClick Flash Cookie Affiliates website visitors  
20 were not provided any information of the identity of Specific Media, nor the  
21 SpecificClick Flash Cookie Affiliates "counter and statistic tracker" entity within  
22 SpecificClick Flash Cookie Affiliates' Terms of Service and Privacy Policy.

23 45. In addition to the SpecificClick Flash Cookie Affiliates and Specific  
24 Media privacy documents, a user would be obligated to review their Flash media  
25 player's privacy documents. Some Internet users possess multiple Flash media  
26 players, and many are not aware of the identity of their Flash media player nor are  
27 provided information from Defendant as to the identity of the Flash media player  
28 being apprehended for use by the SpecificClick Flash Cookie Affiliates and/or



1 Specific Media. If a user could identify their involved Flash media player, and the  
2 identity of the corporate entity for the Flash media player, the user would have  
3 additional obligations imposed upon them to download, read, and comprehend the  
4 Flash media player's privacy documents, such as Adobe's, the largest Flash media  
5 player provider.

6 46. SpecificClick Flash Cookie Affiliates' users' online privacy  
7 protection was premised upon imposed requirement to download, read and  
8 comprehend the accumulation of all privacy documents of SpecificClick Flash  
9 Cookie Affiliates, Specific Media, and the user's Flash media player, such as  
10 Adobe.

11 47. A millisecond was the time allotted to an online visitor opening a  
12 SpecificClick Flash Cookie Affiliates' webpage, before a Flash cookie was  
13 embedded within their computer and data collected immediately, without their  
14 awareness, knowledge or consent to such actions. Such occurred without the  
15 benefit of being provided adequate time to access, read, and attempt to  
16 comprehend the Terms of Service/Use and Privacy Policy for SpecificClick Flash  
17 Cookie Affiliates' website, Specific Media's, and the website of the user's Flash  
18 media player. While only the most technical savvy online users were familiar with  
19 cookies, a finite amount of individuals even knew about Flash cookies, let alone  
20 could possibly comprehend the technical aspects of Flash cookies inherent within  
21 the Defendant's privacy documents.

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

26 *"There was of course no way of knowing whether you were being*  
27 *watched at any given moment. How often, or on what system, the*  
28 *Thought Police plugged in on any individual wire was guesswork.*  
*It was even conceivable that they watched everybody all the time.*

1                   *But at any rate they could plug in your wire whenever they wanted*  
2                   *to. You had to live—did live, from habit that became instinct—in*  
3                   *the assumption that every sound you made was overheard, and,*  
4                   *except in darkness, every movement scrutinized.”*

## 5                   **STATEMENT OF FACTS**

### 6                   **A. Background**

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

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

28                   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](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862).

1        **B. Traditional Online Advertising**

2            50. Commercial websites, such as SpecificClick Flash Cookie Affiliates,  
3 use online advertising in order to promote content to the consumers without charge  
4 and require online advertising to support this objective. Commercial websites,  
5 known as “publishers” allow portions of their web page to be sold to online  
6 advertising networks, which act as an intermediary between “publishers” and the  
7 “advertisers.”

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

13           52. Web advertisements provided by “third-party ad servers” inject their  
14 advertisements into hosting web pages. The web page upon which an  
15 advertisement will appear reserves a blank space in the page's layout with a URL  
16 containing a third-party advertising server address. Whenever that page is  
17 displayed, the user's web browser will read the page, discover the URL address of  
18 the advertising server, and request a web page asset from it. This could be an  
19 image, Flash animation, video, or other resource from the third-party server. When  
20 the advertising asset is received by the browser, it will be inserted into the page to  
21 appear in the reserved location and become part of the delivered page.

22           53. Publishers desiring to identify and track users while they were on their  
23 site embed “first party” tracking devices, “session cookies,” used to facilitate a  
24 user’s activities within the selected website while actively on that site, and  
25 “persistent cookies,” which exist beyond the period of the initial website session  
26 and provides tracking technology while a user visits all websites.

27           54. Online advertising companies use a tracking system to gauge  
28 webpages as activity while the user navigated online in and out of its advertising

1 network, and “third-party cookies” accomplish this goal. In the process of  
2 advertising placement/injection, advertisers can place cookies on the user’s  
3 machine. Since the advertisers place ads on multiple sites, the cookie allows the  
4 advertiser to observe the user’s browsing behavior across many websites. Large  
5 ad-serving agents span significant portions of the World Wide Web and thereby  
6 acquire extensive behavioral data. The net result is that the user gets a cookie from  
7 the media service without ever having visited it.

8         55. Cookies typically are small files. The cookie text files themselves  
9 consist of strings of “name-value” pairs that reduce to code various pieces of  
10 information about an individual’s computer, the browsing choices a person makes  
11 while accessing a Web site and any additional information a person discloses  
12 during a particular visit. While some cookies may contain minimal information,  
13 others may record a wide array of user-profiling information, IP numbers,  
14 shopping cart contents, user IDs, user-selected preferences, serial numbers,  
15 frequencies of contact with companies, demographics, purchasing histories, credit-  
16 worthiness, social security numbers and other personal identifiers, credit card  
17 numbers, phone numbers, and addresses. In addition to that user specific  
18 information, the name-value pairs include basic parameters regarding the range of  
19 servers and sites that can access the cookie from an individual’s hard drive as well  
20 as the cookie expiration date.

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

25         57. Cookies are based on a two-stage process. First the cookie is stored in  
26 the user's computer. The web server creates a specific cookie, which is essentially a  
27 string of text containing the user's preferences, and it transmits this cookie to the  
28 user's computer. The user's web browser receives the cookie and stores it on the

1 computer. As a result, personal information is formatted by the web server,  
2 transmitted, and saved by the user's computer.

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

8 59. Cookies are normally only sent to the server setting them or a server  
9 in the same domain (e.g., a cookie set by mail.abc.com could be shared with  
10 calendar.abc.com). These are called first-party cookies because they are set by the  
11 site displayed in the address bar of the Web browser. Third-party cookies, on the  
12 other hand, are typically used by advertising networks to track users across  
13 multiple websites where the networks have placed advertising—which allows the  
14 advertising network to target subsequent advertisements to the user's presumed  
15 interests and also to limit the number of times a user is shown a particular ad.

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

1 across sessions. For this reason, cookies with a date is expiration dates are referred  
2 to as “persistent” cookies.

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

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

11 63. Clickstream data may include basic information, such as the type of  
12 computer an individual used to access the Internet, the kind of Internet browser  
13 utilized and the identification of each site or page visited. In addition, were an  
14 individual to disclose certain information during the visit, the clickstream data may  
15 also include more personalized details, such as passwords, e-mail addresses, credit  
16 card numbers, name, address, date of birth, gender, or zip code.

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

1           **C. Web Browser Preferences**

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

8           66. Individuals have a reasonable expectation of privacy in their personal  
9 computer, the integrity of their computers, and the confidentiality of their  
10 communications with the Internet websites that they visit, using their Internet  
11 connection to transmit and receive personal and private data, including but not  
12 limited to, personal emails, personal Internet research and viewing, credit card  
13 information, banking information, personal identifiable information such as social  
14 security number, date of birth, and medical information.

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

24           68. Browser cookie controls and preference settings provide greater user  
25 privacy control. The purpose of a browser privacy mode is to allow users to browse  
26 the Internet without leaving data tracks. Browsers save visited websites in the  
27 browsing history, downloaded files in the download history, search terms in the  
28 search history, and data typed into online registration forms including cached

1 version of such files. Cookie controls allow the user to decide which cookies can  
2 be stored on their computer and transmitted to websites, and using parental  
3 controls to block specific content by adjusting the tabs located within the user's  
4 browser.

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

8 *“Contrary to what many marketers claim, most adult Americans*  
9 *(66%) do not want marketers to tailor advertisements to their*  
10 *interests. Moreover, when Americans are informed of three common*  
11 *ways that marketers gather data about people in order to tailor ads,*  
12 *even higher percentages - between 73% and 86% - say they would not*  
13 *want such advertising.”*

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

#### 17 **D. Flash Player- Cookies-LSO**

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

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



1 domain's directory, you will eventually find a "SOL" file. This file contains the  
2 data that is stored and used as the Flash cookie.

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

7 73. Functionally, client storage areas are quite different from cookies.  
8 DOM Storage doesn't transmit values to the server with every request as cookies  
9 do, nor does the data in a local storage area ever expire. And unlike cookies, it is  
10 easy to access individual pieces of data using a standard interface that has growing  
11 support among browser vendors. If objects are stored in a Local Object Repository  
12 then these are available to specific actions but not to all the actions. But if these  
13 objects are stored in one or more Shared Object Repositories then multiple actions  
14 or tests can use them.

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

24 75. Flash LSO cookies properties:

- 25 • SOL files are stored outside of the browser's cache, and removed  
26 when a web browser's cache is cleared.
- 27 • By default they offer storage of 100 KB (compare: Usual cookies 4  
28 KB).
- Browsers are not aware of Flash cookies, and LSO's usually cannot be

1 removed by browsers.

- 2 ● Flash can access and store highly specific personal and technical  
3 information (system, user name, files...).
- 4 ● Ability to send the stored information to the appropriate server,  
5 without user's permission.
- 6 ● Flash applications do not need to be visible
- 7 ● There is no easy way to tell which Flash-cookie sites are tracking you.
- 8 ● Shared folders allow cross-browser tracking
- 9 ● There is currently no mechanism to force a shared-object to "expire".  
10 Browser cookies have an expiration mechanism built in.
- 11 ● User can only disable local shared-object by disallowing a particular  
12 site to write to the user's hard drive. This can be done in the  
13 Macromedia player Setting window.

14 76. Since Flash runs independently from the browser, it needs its own  
15 temporary storage area for web sites to store information related to the Flash  
16 movie, saving objects, in either the local and shared object repositories. The data is  
17 split into two folders: "#SharedObjects" and "macromedia.com". The content  
18 located inside the "macromedia.com" is set by the site and controls settings for the  
19 site visited, while the content located inside "#SharedObjects" is created by the site  
20 visited or a third party company and contains the cookie values we are researching.

21 77. Defendant's Flash cookie setting process was a system, method and  
22 computer readable medium configured to track Internet users as they browse web-  
23 sites when cookies are disabled or deleted. Defendant SpecificClick Flash Cookie  
24 Affiliate's website receives a request for content from the computing-device. After  
25 obtaining information about the computing-device, the tracking-server assesses the  
26 request for content from the computing-device. If the computing-device has an  
27 available Flash plug-in, the tracking-server transmits a Flash applet to the  
28 computing-device. The Flash applet is configured to: determine whether a unique  
Flash identifier has been assigned to the computing-device, generate the unique  
Flash identifier if no unique Flash identifier has already been assigned to the  
computing-device, transmit the unique Flash identifier to a tracking server, and

1 store the unique Flash identifier in local Flash storage. The process also stores a  
2 cookie at the computing-device when no Flash plug-in is available.

3 **E. “Flash Cookies and Privacy”- Berkeley Study**

4 78. A study released by researchers at the University of California,  
5 Berkeley and other universities, submitted to the federal government for  
6 consideration as part of a new policy on the use of tracking technologies, revealed  
7 the details of Defendant Specific Media’s online privacy invasion of epidemic  
8 proportions, that reverberated globally.

9 Ashkan Soltani *et al.*, “Flash Cookies and Privacy” (10 August 2009),  
10 online: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1446862](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862).

11 **F. Overlapping Values**

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

15 *“It’s also worth mentioning that ‘\_tpf’ and ‘\_fpf’ were found to also*  
16 *contain unique identifiers which were also found to contain*  
*overlapping values as the ones found in HTML cookies for ‘uid’ or*  
*‘userid.’”*

17 *“Of the top 100 websites, 31 had at least one overlap between a*  
18 *HTTP and Flash cookie. For instance, a website might have an HTTP*  
19 *cookie labeled “uid” with a long value such as 4a7082eb-775d6-*  
20 *d440f-dbf25. There were 41 such matches on these 31 sites. Most*  
21 *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.”*

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

24 80. “Zombie cookies,” or browser cookies that are respawned by Flash  
25 cookies, required a Flash setting file and a directory, labeled by the domain, which  
26 set the Flash cookie. Such created a history of all users’ activities, thus the coding  
27 required was neither inadvertent nor an “unintended effect,” and permitted the  
28

1 Flash cookie to respawn a deleted browser cookie derived from the history data  
2 file:

3 *“Presence of Flash settings files- Each settings is stored in its own*  
4 *directory, labeled by domain. This creates a type of history file*  
5 *parallel to the one created by the browser. However, the Flash history*  
6 *is not deleted when browser controls are used to erase information*  
7 *about sites previously visited. This means that users may falsely believe*  
8 *that they have fully cleared their history when using the standard*  
9 *browser tools.”*

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

13 81. A technical discussion alone of respawning Flash cookies by ad  
14 networks in general, without visualization of such activity, fails to accentuate the  
15 willful and wanton disregard of user’s preferences. Case in point: User’s  
16 preference is to opt-out from having a Flash cookie set, this on 3/21/2010 at  
17 10:18:08 AM evidenced within the log activity as “optout.sol.”

18 `http://core. [name redacted].com/#com/[name redacted]OptOut.sol`  
19 `3/21/2010 10:18:08 AM 3/21/2010 10:18:08 AM 61 C:\Users\[user’s`  
20 `name redacted] \AppData\Roaming\Macromedia\Flash`  
21 `Player\#SharedObjects\3VYPOS2K\core. [name`  
22 `redacted].com/#com/[name redacted]\OptOut.sol`

23 82. User’s Flash cookie preference is disregarded as evidenced within the  
24 log activity as “retargeting.sol.” Such activity occurs within five (5) second on  
25 3/21/2010 10:18:13 AM.

26 `http://core.[name redacted].com/#com/[name redacted].`  
27 `Retargeting.sol 3/21/2010 10:18:13 AM 5/22/2010 9:12:24 AM`  
28 `120 C:\Users\[user’s name redacted]`  
29 `\AppData\Roaming\Macromedia\Flash`  
30 `Player\#SharedObjects\3VYPOS2K\core. [name`  
31 `redacted].com/#com/[name redacted].\Retargeting.sol`

32 83. The expiration date of cookie information and the entropy of the  
33 information contained in the cookie provides limited information. If the entropy is  
34 low (e.g. content is “volume =5”) then it can be assumed to be a legitimate setting  
35 to be saved. If the entropy is high (e.g. “userId = b56574ce78d2f110b1gd522”) then  
36 it is more likely than not a tracking id connected to a background database of

1 user information, i.e. a user goes to a website wherein the algorithm locates a  
2 normal cookie stored by an advertising network, then the algorithm searched for  
3 repeating keys. Every character (at least in a charset like ASCII) counts one byte,  
4 thus counting the number of characters in “id=344499284532” which are 15 and in  
5 “volume\_level=98, language=English” which are 32. The analysis of both HTTP  
6 and Flash cookies for key identifiers revealed undisputable correlations including  
7 overlapping values.

8 84. Researchers were able to identify a high number of cookies similarly  
9 labeled such as: “user ID.” These cookies stored unique identifiers which allowed  
10 user tracking; however unlike HTTP cookies used for tracking these cookies had  
11 overlapping values. This respawning was because of the Flash cookies, provided  
12 by Specific Media, had the same data values as the HTTP cookies, provided by the  
13 SpecificClick Flash Cookie Affiliates, so in effect the Flash cookies acted as a  
14 back-up on the computer systems once the HTTP cookies had been removed. If  
15 users simply deleted cookies without clearing the browser cache, the identifiers in  
16 the deleted browser cookies still returned to the cookies, more than likely, using  
17 information stored in the cache.

18 85. When HTML cookies are deleted, the users would get a new value  
19 when visiting the site. But when Flash cookies and HTML cookies are given the  
20 same value, as they were on 31 of the top 100 websites, “it will restore the value of  
21 your original cookie, and thereby nullifies the deletion of the HTML cookies,”

22 Soltani said

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

26 86. Defendant implanted identical code in the Plaintiffs and Class  
27 Members’ computers resulting in a uniform action to set redundant unique  
28 identifiers used to identify and track users overlapping values.

1  
2 **G. Defendant's Harmful Business Practices**

3 87. Defendant Specific Media's activities with SpecificClick Flash  
4 Cookie Affiliates occurred throughout the United States, and have secretly  
5 obtained personal and private information from Plaintiffs and the Class - a course  
6 of action and a body of information that is protected from interception, access, and  
7 disclosure by federal law.

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

15 89. At all relevant times, Defendant's advertising technology has  
16 contained secret information-gathering capacities that were not disclosed to or  
17 known by Plaintiffs or the Class and which permitted Defendant to surreptitiously,  
18 in an unauthorized manner, and for tortious and unlawful purposes, intercept and  
19 access Plaintiffs' and the Class Members' personal and private information,  
20 monitor their Internet activity, and create detailed personal profiles based on such  
21 information.

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

1 and the contents of any information they provided to or obtained from a particular  
2 website.

3 91. Defendant has used those cookies and other surreptitious data-  
4 collection methods to secretly intercept and access computer users' personal data  
5 and web browsing habits and have transmitted this information to Defendant for its  
6 own commercial benefit.

7 92. Defendant collected and/or disclosed covered information of Class  
8 Members about all or substantially all of their online activity, including across  
9 websites.

10 93. Defendant's business practice unfairly wrests control from users who  
11 choose to delete their cookies in order to avoid being tracked. Advertising  
12 networks use unique IDs to identify the same user or computer across many  
13 different websites. Users who are aware of this may delete their cookies  
14 periodically, believing that the new cookies they receive will contain new unique  
15 identifiers, thus hindering the ability of advertising networks to track their behavior  
16 across sites. Using Flash cookies to re-identify users overrides this control, with  
17 little available redress for users. Although users may arguably protect themselves  
18 by periodically deleting their Flash cookies as well, the means for doing so are  
19 extremely obscure and difficult even for savvy consumers to use. Flash specifically  
20 attempts to obfuscate data within each LSO by controlling the format and forcing a  
21 binary serialization of any stored data, thus bypassing the web browser's same-  
22 origin security policy, allowing an application hosted on one domain to read data  
23 or code hosted on another.

24 94. Defendant failed to disclose that its applied technologies also provide  
25 Defendant with the ability to surreptitiously intercept, access, and collect electronic  
26 communications and information from unsuspecting Internet users—including  
27 Plaintiffs and the Class.

28 95. Defendant intercepted Class Members' electronic communications for

1 the purpose of committing a tortious or criminal act, and violated the constitutional  
2 rights of Plaintiffs and Class Members.

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

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

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

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

16 100. Plaintiffs and the Class Members did not voluntarily disclose their  
17 personal and private information, including their Internet surfing habits, to  
18 Defendant - and indeed never even knew that Defendant existed or conducted data  
19 collection and monitoring activities upon and across its plaintiff and class  
20 member's websites. Plaintiffs and the Class Members provided such information,  
21 and had their Internet habits monitored, without their knowledge or consent, and  
22 would not have consented having their personal and private information, including  
23 their on-line profiles, used for Defendant's commercial gain.

24 101. Defendant did not obtain consent from Plaintiffs and Class Members  
25 for any collection or use and was not allowed to decline consent at the time such  
26 statement was presented to the Class Members.

27 102. Defendant did not obtain consent from Plaintiffs and Class Members  
28 for any disclosure of covered information to unaffiliated parties and was not



1 allowed to decline consent at the time such statement was presented to the Class  
2 Members.

3 103. Defendant has covertly, without consent, and in an unauthorized,  
4 deceptive, invasive, and fraudulent manner implanted Internet “Flash cookies”  
5 upon Internet users’ computer hard disk drives to use its local storage within the  
6 Flash media player to back up browser cookies for the purposes of restoring them  
7 later.

8 104. Defendant intentionally accessed Plaintiffs and Class Members’  
9 computer without authorization or exceeded authorized access to obtain  
10 information from a protected computers, involved an interstate communications.

11 105. Defendant sold, shared, and/or otherwise disclosed covered  
12 information of Class Members to an unaffiliated party without first obtaining the  
13 consent of the Class Members to whom the covered information related to.

14 106. At all relevant times, Plaintiffs and Class Members’ personal and  
15 private information was intercepted by and/or accessed by Defendant and  
16 transmitted to it on a regular basis, without alerting Internet users in any manner.  
17 As a result, Defendant was able to and did access Plaintiffs’ and Class Members’  
18 computer systems and/or intercept their electronic communications without  
19 authorization. Defendant has obtained, compiled, and used this personal  
20 information for its own commercial purposes.

21 107. Defendant intercepted Class Members’ electronic communications for  
22 the purposes of implanting unauthorized Flash cookies on Class Members’  
23 computers; repeatedly accessing electronic communications without Class  
24 Members’ knowledge and consent so as to profile such persons’ web browsing  
25 habits, secretly tracking Class Members’ activities on the Internet and collecting  
26 personal information about consumers; and profiting from the use of the illegally  
27 obtained information, all to Defendant’s benefit and Class Members’ detriment.

28 108. Defendant intentionally intercepted, endeavored to intercept, or

1 procured another person to intercept or endeavor to intercept the electronic  
2 communication of Plaintiffs and Class Members.

3 109. Defendant has, either directly or by aiding, abetting and/or conspiring  
4 to do so, knowingly, recklessly, or negligently disclosed, exploited,  
5 misappropriated and/or engaged in widespread commercial usage of Plaintiffs' and  
6 the Class' private and sensitive information for Defendant's own benefit without  
7 Plaintiffs' or the Class' knowledge, authorization, or consent. Such conduct  
8 constitutes a highly offensive and dangerous invasion of Plaintiffs' and the Class'  
9 privacy.

10 110. Defendant used and consumed the resources of the Plaintiffs and  
11 Class Members' computers and substantially increased their Internet bandwidth by  
12 gathering user information and transferring such to Defendant.

13 111. Defendant caused harm and damages to Plaintiffs and Class  
14 Members' computers finite resources, depleted and exhausted its memory, thus  
15 causing an actual inability to use it for its intended purposes, and significant  
16 unwanted CPU activity, disk usage, and network traffic resulting in instability  
17 issues, such as applications freezing, failure to boot, and system-wide crashes.

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

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

25 114. Defendant's downloads were not evident. Users assumed that the  
26 issues relate to hardware, Windows installation problems, or another infection, and  
27 resorted to contacting technical support experts, or even buying a new computer  
28 because the existing system "has become too slow." Class Members attempting to

1 repair their own computer risked damaging their system files. Badly infected  
2 systems required a clean reinstallation of all their software in order to return to full  
3 functionality, with charges of a few hundred dollars to remove viruses and  
4 spyware, and unauthorized Flash cookies, if serviced in house, or on site such costs  
5 exceeded \$40-\$60 per hour.

6 115. Defendant harmed Plaintiffs and Class Members by its actions which  
7 included, but not limited to the following:

- 8 a) Loss of valuable data by attempts to remove Flash cookies once  
9 discovered;
- 10 b) Incurred economic losses accompanied by an interruption in service;
- 11 c) Functionality of computer interfered with, including an inability of  
12 websites visited once Flash content was disabled;
- 13 d) Information was deleted, otherwise made unavailable;
- 14 e) Impaired the integrity and availability of data, programs and  
15 information.

16 116. Defendant Specific Media and SpecificClick Flash Cookie Affiliates'  
17 technology wrongfully monitored Internet users' activities at each and every  
18 website users visited at which Defendant's products or services were not utilized.  
19 The wrongfulness of this conduct is multiplied by the fact that Defendant  
20 aggregates this information about users' habits across numerous websites and  
21 unjustly enriched Defendant to the severe detriment of Plaintiffs and the Class.  
22 Plaintiffs and the Class have been harmed, as they have been subjected to repeated  
23 and unauthorized invasions of their privacy - violations which continue to this day.

24 117. The collection of data by Defendant was wholesale and all-  
25 encompassing. Data passing from the users' computers were acquired by  
26 Defendant without discrimination as to the kind, type, nature, or sensitivity of the  
27 data. Like the privacy one loses from an airport security body scanner, everything  
28 passing through the consumer's Internet connection was intercepted by Defendant,  
claimed as their property, and traded as a commodity. Regardless of any

1 representations to the contrary—all data—whether sensitive, financial, personal,  
2 private, complete with all identifying information, was intercepted, exposing users  
3 like “fish in a fishbowl.”

4 **CLASS ALLEGATIONS**  
5 **Allegations as to Class Certification**

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

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

27 119. The Class action period, (the “Class Period”), pertains to the date, two  
28 years preceding the date of this filing to the date of Class certification.

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

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

- a) Computer Fraud and Abuse Act (“CFAA”),

- 1  
2  
3
- b) California's Computer Crime Law, ("CCCL"),
  - c) Trespass to Personal Property / Chattels, and
  - d) Unjust Enrichment

4 All persons residing in United States who, during the period of  
5 two years preceding the date of this filing to the date of Class  
6 certification (the "Class Period"), accessed a SpecificClick Flash  
7 Cookie Affiliate website and had a Defendant flash cookie set  
8 on their computer to use its local storage within the Flash media  
9 player to back up browser cookies for the purposes of restoring  
10 them later.  
11 (hereinafter referred to as "CFAA/ CCCL SubClass.")

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

- 15
- a) California's Computer Crime Law ("CCCL"),
  - b) California's Invasion of Privacy Act,
  - c) Violation of California's Consumer Legal Remedies Act, Civil Code § 1750;
  - d) Violation of California's Unfair Competition Law, Business and Professions Code § 17200,

16 All persons residing in United States who, during the Class  
17 period, and accessed a SpecificClick Flash Cookie Affiliate  
18 website and had a Defendant flash cookie set on their computer  
19 to use its local storage within the Flash media player to back up  
20 browser cookies for the purposes of restoring them later.  
21 (hereinafter referred to as "California Resident Class.")

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

- 24
- a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
  - b) California's Computer Crime Law, Penal Code § 502;
  - c) California Invasion Of Privacy Act, California Penal Code § 630;
  - d) Violation of California's Consumer Legal Remedies Act, Civil Code § 1750;
  - e) Violation of California's Unfair Competition Law, Business and Professions Code § 17200;
  - f) Trespass to Personal Property / Chattels;
- 26  
27  
28

g) Unjust Enrichment

1  
2 124. On behalf of the Injunctive Class, Plaintiffs seek only injunctive  
3 relief.

4 125. **Persons Excluded From Classes:** Subject to additional information  
5 obtained through further investigation and discovery, the foregoing definition of  
6 the Class may be expanded or narrowed by amendment or amended complaint.  
7 Specifically excluded from the proposed Class are Defendant, their officers,  
8 directors, agents, trustees, parents, children, corporations, trusts, representatives,  
9 employees, principals, servants, partners, joint venturers, or entities controlled by  
10 Defendant, and their heirs, successors, assigns, or other persons or entities related  
11 to or affiliated with Defendant and/or their officers and/or directors, or any of  
12 them; the Judge assigned to this action, and any member of the Judge's immediate  
13 family.

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

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

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

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

- a) What was the extent of Defendant Specific Media and SpecificClick Flash Cookie Affiliates' business practice of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later and how did it work?
- b) What information did Defendant Specific Media and SpecificClick Flash Cookie Affiliates' collect from its business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later, and what did it do with that information?
- c) Whether SpecificClick Flash Cookie Affiliate users, by virtue of their visitation to SpecificClick Flash Cookie Affiliate's website, had pre-consented to the operation of Specific Media and SpecificClick 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 Defendant Specific Media and SpecificClick Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later provided to Defendant Specific Media and SpecificClick Flash Cookie Affiliates' users?
- e) Was there reasonable opportunity to decline the operation of Defendant Specific Media and SpecificClick Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later provided to Defendant Specific Media and SpecificClick Flash Cookie Affiliates' users?
- f) Did Defendant Specific Media and SpecificClick Flash Cookie Affiliates' business practices of setting a Flash cookie on a user's computer to use its local storage within the Flash media player to back up browser cookies for the purpose of restoring them later disclose, intercept, and transmit personally identifying information, or sensitive identifying information, or personal information?
- g) Whether Defendant Specific Media and SpecificClick Flash Cookie Affiliates devised and deployed a scheme or artifice to defraud or conceal from Plaintiffs and the Class Defendant Specific Media and SpecificClick Flash Cookie Affiliates' ability to, and practice of, intercepting, accessing, and manipulating, for its own benefit, personal information, and tracking data from Plaintiffs' and the Class' personal computers via the ability to; (and practice of) implanting secret "cookies" on their computers;
- h) Whether Defendant Specific Media and SpecificClick Flash

1 Cookie Affiliates engaged in deceptive acts and practices in,  
2 connection with its undisclosed and systemic practice of  
3 implanting, accessing and/or disclosing unique identifiers, tracking  
4 data, and personal information on Plaintiffs and the Class' personal  
5 computers and using that data to track and profile Plaintiffs' and  
6 the Class' Internet activities and personal habits, proclivities,  
7 tendencies, and preferences for Defendant's use and benefit;

- 8 i) Did the implementation of Defendant Specific Media and  
9 SpecificClick Flash Cookie Affiliates' business practices of setting  
10 a Flash cookie on a user's computer to use its local storage within  
11 the Flash media player to back up browser cookies for the purpose  
12 of restoring them later violate the Computer Fraud and Abuse Act,  
13 18 U.S.C. §§ 1030?
- 14 j) Did the operation, function, and/or implementation of Defendant  
15 Specific Media and SpecificClick Flash Cookie Affiliates'  
16 business practices of setting a Flash cookie on a user's computer to  
17 use its local storage within the Flash media player to back up  
18 browser cookies for the purpose of restoring them later violate  
19 California's Computer Crime Law, California Penal Code § 502?
- 20 k) Did the operation, function, and/or implementation of Defendant  
21 Specific Media and SpecificClick Flash Cookie Affiliates'  
22 business practices of setting a Flash cookie on a user's computer to  
23 use its local storage within the Flash media player to back up  
24 browser cookies for the purpose of restoring them later violate the  
25 California Invasion of Privacy Act, California Penal Code § 630?
- 26 l) Did the operation, function, and/or implementation of Defendant  
27 Specific Media and SpecificClick Flash Cookie Affiliates'  
28 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 Defendant herein?
- m) Are the Defendant Specific Media and/or SpecificClick Flash  
Cookie Affiliates liable under a theory of aiding and abetting for  
violations of the statutes listed herein?
- n) Are the Defendant Specific Media and/or SpecificClick Flash  
Cookie Affiliates liable under a theory of civil conspiracy for  
violations of the statutes listed herein?
- o) Are the Defendant Specific Media and/or SpecificClick Flash  
Cookie Affiliates liable under a theory of unjust enrichment for  
violations of the statutes listed herein?
- p) Whether Defendant Specific Media and SpecificClick 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 Defendant Specific Media and SpecificClick  
Flash Cookie Affiliates' marketing scheme, and, if so, what is the  
measure of those damages?



- 1 r) Whether Plaintiffs and members of the Class have sustained  
2 damages as a result of Defendant's conduct, and, if so, what is the  
3 appropriate measure of damages;
- 4 s) Whether Plaintiffs and members of the Class are entitled to  
5 declaratory and/or injunctive relief to enjoin the unlawful conduct  
6 alleged herein; and
- 7 t) Whether Plaintiffs and members of the Class are entitled to  
8 punitive damages, and, if so, in what amount.

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

14 130. **Adequacy of Representation:** Plaintiffs will fairly and adequately  
15 protect the interests of the members of the Class. Plaintiffs have retained counsel  
16 highly experienced in complex consumer Class action litigation, and Plaintiffs  
17 intend to prosecute this action vigorously. Plaintiffs have no adverse or  
18 antagonistic interests to those of the Class.

19 131. **Superiority:** A Class action is superior to all other available means  
20 for the fair and efficient adjudication of this controversy. The damages or other  
21 financial detriment suffered by individual Class Members is relatively small  
22 compared to the burden and expense that would be entailed by individual litigation  
23 of their claims against the Defendant. It would thus be virtually impossible for the  
24 Class, on an individual basis, to obtain effective redress for the wrongs done to  
25 them. Furthermore, even if Class Members could afford such individualized  
26 litigation, the court system could not. Individualized litigation would create the  
27 danger of inconsistent or contradictory judgments arising from the same set of  
28 facts. Individualized litigation would also increase the delay and expense to all  
parties and the court system from the issues raised by this action. By contrast, the

1 Class action device provides the benefits of adjudication of these issues in a single  
2 proceeding, economies of scale, and comprehensive supervision by a single court,  
3 and presents no unusual management difficulties under the circumstances here.

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

- 5 a) the prosecution of separate actions by individual Class Members  
6 would create a risk of inconsistent or varying adjudication with  
7 respect to individual Class Members that would establish  
8 incompatible standards of conduct for the Defendant;
- 9 b) the prosecution of separate actions by individual Class Members  
10 would create a risk of adjudications with respect to them that  
11 would, as a practical matter, be dispositive of the interests of other  
12 Class Members not parties to the adjudications, or substantially  
13 impair or impede their ability to protect their interests; and/or
- 14 c) Defendant have acted or refused to act on grounds generally  
15 applicable to the Class thereby making appropriate final  
16 declaratory and/or injunctive relief with respect to the members of  
17 the Class as a whole.

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

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

24 135. Adequate notice can be given to Class Members directly using  
25 information maintained in Defendant's records, or through notice by publication.

26 136. Damages may be calculated from the information maintained in  
27 Defendant's records, so that the cost of administering a recovery for the Class can  
28 be minimized. The amount of damages is known with precision from Defendant's  
records.

**Count I**  
**Violation of the Computer Fraud and Abuse Act**  
**18 U.S.C. § 1030 et seq.**  
**By All Plaintiffs against Defendant**

1  
2  
3  
4 137. Plaintiffs incorporate the above allegations by reference as if set forth  
5 herein at length.

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

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

14 140. Defendant violated 18 U.S.C. § 1030 by intentionally accessing a  
15 Plaintiffs’ computer, without authorization or by exceeding access, thereby  
16 obtaining information from such a protected computer.

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

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

25 143. Plaintiffs’ computer is a “protected computer...which is used in  
26 interstate commerce and/or communication” within the meaning of 18 U.S.C. §  
27 1030(e)(2)(B).

28 144. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by intentionally

1 accessing a Plaintiffs' computer, without authorization or by exceeding access,  
2 thereby obtaining information from such a protected computer.

3 145. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly  
4 causing the transmission of a command embedded within their webpages,  
5 downloaded to Plaintiffs' computer, which are protected computers as defined in  
6 18 U.S.C. § 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs'  
7 viewing habits, Defendant intentionally caused damage without authorization to  
8 those Plaintiffs' computers by impairing the integrity of the computer.

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

14 147. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally  
15 accessing Plaintiffs and Class Members' protected computers without  
16 authorization, and as a result of such conduct, caused damage and loss to Plaintiffs  
17 and Class Members.

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

21 149. Plaintiffs have suffered loss by reason of these violations, as defined  
22 in 18 U.S.C. § 1030(e)(11), by the "reasonable cost ... including the cost of  
23 responding to an offense, conducting a damage assessment, and restoring the data,  
24 program, system, or information to its condition prior to the offense, and any  
25 revenue lost, cost incurred, or other consequential damages incurred because of  
26 interruption of service."

27 150. Plaintiffs have suffered loss by reason of these violations, including,  
28 without limitation, violation of the right of privacy, disclosure of personal

1 indentifying information, sensitive identifying information, and personal  
2 information, interception, and transactional information that otherwise is private,  
3 confidential, and not of public record.

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

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

10 153. Defendant's unlawful access to Plaintiffs' computers and electronic  
11 communications has caused Plaintiffs irreparable injury. Unless restrained and  
12 enjoined, Defendant will continue to commit such acts. Plaintiffs' remedy at law is  
13 not adequate to compensate it for these inflicted and threatened injuries, entitling  
14 Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C. §  
15 1030(g).

16 **Count II**  
17 **Violation of California's Computer Crime Law ("CCCL")**  
18 **California Penal Code § 502**  
19 **By All Plaintiffs against Defendant**

20 154. Plaintiffs incorporate the above allegations by reference as if set forth  
21 herein at length.

22 155. Plaintiffs assert this claim against Defendant named herein in this  
23 complaint on behalf of themselves and the Class.

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

27 157. Defendant violated California Penal Code § 502 by knowingly  
28 accessing, copying, using, made use of, interfering, and/or altering, data belonging

1 to Plaintiffs and Class Members: (1) in and from the State of California; (2) in the  
2 home states of the Plaintiffs; and (3) in the state in which the servers that provided  
3 the communication link between Plaintiffs and the websites they interacted with  
4 were located.

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

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

13 160. Pursuant to California Penal Code § 502(b)(8), “Injury means any  
14 alteration, deletion, damage, or destruction of a computer system, computer  
15 network, computer program, or data caused by the access, or the denial of access to  
16 legitimate users of a computer system, network, or program.”

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

27 162. Defendant has violated California Penal Code § 502(c)(1) by  
28 knowingly accessing and without permission, altering, and making use of data

1 from Plaintiffs' computers in order to device and execute business practices to  
2 deceive Plaintiffs and Class Members into surrendering private electronic  
3 communications and activities for Defendant's financial gain, and to wrongfully  
4 obtain valuable private data from Plaintiffs.

5 163. Defendant has violated California Penal Code § 502(c)(2) by  
6 knowingly accessing and without permission, taking, or making use of data from  
7 Plaintiffs' computers.

8 164. Defendant has violated California Penal Code § 502(c)(3) by  
9 knowingly and without permission, using and causing to be used Plaintiffs'  
10 computer services.

11 165. Defendant has violated California Penal Code § 502(c)(4) by  
12 knowingly accessing and without permission, adding and/or altering the data from  
13 Plaintiffs' computers.

14 166. Defendant has violated California Penal Code § 502(c)(5) by  
15 knowingly and without permission, disrupting or causing the disruption of  
16 Plaintiffs' computer services or denying or causing the denial of computer services  
17 to Plaintiffs.

18 167. Defendant has violated California Penal Code § 502(c)(6) by  
19 knowingly and without permission providing, or assisting in providing, a means of  
20 accessing Plaintiffs' computers, computer system, and/or computer network.

21 168. Defendant has violated California Penal Code § 502(c)(7) by  
22 knowingly and without permission accessing, or causing to be accessed, Plaintiffs'  
23 computer, computer system, and/or computer network.

24 169. Defendant has violated California Penal Code § 502(c)(8) by  
25 knowingly introducing a computer contaminant into the Plaintiffs' computer,  
26 computer system and/or computer network to obtain data regarding Plaintiffs'  
27 electronic communications.

28 170. California Penal Code § 502(j) states: "For purposes of bringing a

1 civil or a criminal action under this section, a person who causes, by any means,  
2 the access of a computer, computer system, or computer network in one  
3 jurisdiction from another jurisdiction is deemed to have personally accessed the  
4 computer, computer system, or computer network in each jurisdiction.”

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

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

14 173. As a direct and proximate result of Defendant’s unlawful conduct  
15 within the meaning of California Penal Code § 502, Defendant has caused loss to  
16 Plaintiffs in an amount to be proven at trial. Plaintiffs are also entitled to recover  
17 their reasonable attorneys’ fees pursuant to California Penal Code § 502(e).

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

20 175. Plaintiffs and Class Members have suffered irreparable and  
21 incalculable harm and injuries from Defendant’s violations. The harm will  
22 continue unless Defendant is enjoined from further violations of this section.  
23 Plaintiffs and Class Members have no adequate remedy at law.

24 176. Plaintiffs and the Class Members are entitled to punitive or exemplary  
25 damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant’s violation  
26 were willful and, on information and belief, Defendant is guilty of oppression,  
27 fraud, or malice as defined in Cal. Civil Code § 3294.

28 177. Defendant’s unlawful access to Plaintiffs’ computers and electronic



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

6 **Count III**  
7 **Violation of the California Invasion of Privacy Act**  
8 **Penal Code section 630 et seq.**  
9 **By All Plaintiffs against Defendant**

10 178. Plaintiffs incorporate the above allegations by reference as if set forth  
11 herein at length.

12 179. Plaintiffs assert this claim against the California Defendant named  
13 herein in this complaint on behalf of themselves and the Class.

14 180. California Penal Code section 630 provides, in part:

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

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

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

1 web-based entities from Plaintiffs and Class Members were sent to California.

2 183. Plaintiffs and Class Members did not consent to any of the  
3 Defendant's actions in intercepting, reading, and/or learning the contents of their  
4 communications with such California-based entities.

5 184. Plaintiffs and Class Members did not consent to any of the  
6 Defendant's actions in using the contents of their communications with such  
7 California-based entities.

8 185. Defendant is not a "public utility engaged in the business of providing  
9 communications services and facilities . . ."

10 186. The actions alleged herein by the Defendant was not undertaken: "for  
11 the purpose of construction, maintenance, conduct or operation of the services and  
12 facilities of the public utility."

13 187. The actions alleged herein by the Defendant was not undertaken in  
14 connection with: "the use of any instrument, equipment, facility, or service  
15 furnished and used pursuant to the tariffs of a public utility."

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

19 189. The Defendant directly participated in the interception, reading,  
20 and/or learning the contents of the communications between Plaintiffs, Class  
21 Members and California-based web entities.

22 190. Alternatively, and of equal violation of the California Invasion of  
23 Privacy Act, the Defendant aided, agreed with, and/or conspired with Specific  
24 Media to unlawfully do, or permit, or cause to be done all of the acts complained  
25 of herein.

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

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

6 **COUNT IV**  
7 **Violations of the Consumer Legal Remedies Act**  
8 **(“CLRA”) California Civil Code § 1750, et seq.**  
9 **By All Plaintiffs against Defendant**

10 193. Plaintiffs incorporate the foregoing allegations as if fully set forth  
11 herein.

12 194. In violation of Civil Code section 1750, et seq. (the “CLRA”),  
13 Defendant has engaged and is engaging in unfair and deceptive acts and practices  
14 in the course of transactions with Plaintiffs, and such transactions are intended to  
15 and have resulted in the sales of services to consumers. Plaintiffs and the Class  
16 Members are “consumers” as that term is used in the CLRA because they sought or  
17 acquired Defendant’s good or services for personal, family, or household purposes.  
18 Defendant’s past and ongoing acts and practices include but are not limited to:

- 19 a) Defendant’s representations that their services have  
20 characteristics, uses, and benefits that they do not have, in  
21 violation of Civil Code § 1770(a)(5);  
22 b) Defendant’s representations that their services are of a particular  
23 standard, quality and grade but are of another standard quality and  
24 grade, in violation of Civil Codes § 1770(a)(7); and  
25 c) Defendant’s advertisement of services with the intent not to sell  
26 those services as advertised, in violation of Civil Code §  
27 1770(a)(9).

28 195. Defendant’s violations of Civil Code § 1770 have caused damage to  
Plaintiffs and the other Class Members and threaten additional injury if the

1 violations continue. This damage includes the losses set forth above.

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

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

11 **COUNT V**

12 **Violations of the Unfair Competition Law ("UCL") California  
13 Business and Professions Code § 17200, et seq.**

14 **By All Plaintiffs against Defendant**

15 198. Plaintiffs incorporate the foregoing allegations as if fully set forth  
16 herein.

17 199. In violation of California Business and Professions Code § 17200 et  
18 seq., Defendant's conduct in this regard is ongoing and includes, but is not limited  
19 to, unfair, unlawful and fraudulent conduct.

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

24 201. Defendant's business acts and practices are unlawful, in part, because  
25 they violate California Business and Professions Code § 17500, et seq., which  
26 prohibits false advertising, in that they were untrue and misleading statements  
27 relating to Defendant's performance of services and with the intent to induce  
28 consumers to enter into obligations relating to such services, and regarding  
statements Defendant knew were false or by the exercise of reasonable care

1 Defendants should have known to be untrue and misleading.

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

7       203. Defendant's business acts and practices are unfair because they cause  
8 harm and injury-in-fact to Plaintiffs and Class Members and for which Defendant  
9 has no justification other than to increase, beyond what Defendant would have  
10 otherwise realized, their profit in fees from advertisers and their information assets  
11 through the acquisition of consumers' personal information. Defendant's conduct  
12 lacks reasonable and legitimate justification in that Defendant has benefited from  
13 such conduct and practices while Plaintiffs and the Class Members have been  
14 misled as to the nature and integrity of Defendant's services and have, in fact,  
15 suffered material disadvantage regarding their interests in the privacy and  
16 confidentiality of their personal information. Defendant's conduct offends public  
17 policy in California tethered to the Consumer Legal Remedies Act, the state  
18 constitutional right of privacy, and California statutes recognizing the need for  
19 consumers to obtain material information that enables them to safeguard their own  
20 privacy interests, including California Civil Code, Section 1798.80.

21       204. In addition, Defendant's modus operandi constitutes a sharp practice  
22 in that Defendant knew, or should have known, that consumers care about the  
23 status of personal information and email privacy but were unlikely to be aware of  
24 the manner in which Defendant failed to fulfill their commitments to respect  
25 consumers' privacy. Defendant is therefore in violation of the "unfair" prong of the  
26 UCL.

27       205. Defendant's acts and practices were fraudulent within the meaning of  
28 the UCL because they are likely to mislead the members of the public to whom

1 they were directed.

2 **Count VI**  
3 **Trespass to Personal Property / Chattels**  
4 **By All Plaintiffs against Defendant**

5 206. Plaintiffs incorporate by reference and reallege all paragraphs  
6 previously alleged herein.

7 207. The common law prohibits the intentional intermeddling with  
8 personal property, including a computer, in possession of another that results in the  
9 deprivation of the use of the personal property or impairment of the condition,  
10 quality, or usefulness of the personal property.

11 208. By engaging in the acts alleged in this complaint without the  
12 authorization or consent of Plaintiffs and Class Members, Defendant dispossessed  
13 Plaintiffs and Class Members from use and/or access to their computers, or parts of  
14 them. Further, these acts impaired the use, value, and quality of Plaintiffs' and  
15 Class Members' computers. Defendant's acts constituted an intentional  
16 interference with the use and enjoyment of the computers. By the acts described  
17 above, Defendants, has repeatedly and persistently engaged in trespass to personal  
18 property in violation of the common law.

19 209. Without Plaintiffs' and Class Members' consent, or in excess of any  
20 consent given, Defendant knowingly and intentionally accessed Plaintiffs' and  
21 Class Members' property, thereby intermeddling with Plaintiffs' and Class  
22 Members' right to possession of the property and causing injury to Plaintiffs and  
23 the members of the Class.

24 210. Defendant engaged in deception and concealment in order to gain  
25 access to Plaintiffs and Class Members' computers.

26 211. Defendant undertook the following actions with respect to Plaintiffs'  
27 and Class Members' computer:

28 a) Defendant accessed and obtained control over the user's

1 computer;

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

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

7 212. All these acts described above were acts in excess of any authority  
8 any user granted when he or she visited the SpecificClick Flash Cookie Affiliates'  
9 websites and none of these acts was in furtherance of users viewing the  
10 SpecificClick Flash Cookie Affiliates websites. By engaging in deception and  
11 misrepresentation, whatever authority or permission Plaintiffs and Class Members  
12 may have granted to SpecificClick Flash Cookie Affiliates was vitiated.

13 213. Defendant's installation and operation of its program used, interfered,  
14 and/or intermeddled with Plaintiffs' and Class Members' computer systems. Such  
15 use, interference and/or intermeddling was without Class Members' consent or, in  
16 the alternative, in excess of Plaintiffs' and Class Members' consent.

17 214. Defendant's installation and operation of its program constitutes  
18 trespass, nuisance, and an interference with Class Members' chattels, to wit, their  
19 computers.

20 215. Defendant's installation and operation of its program impaired the  
21 condition and value of Class Members' computers.

22 216. Defendant's trespass to chattels, nuisance, and interference caused  
23 real and substantial damage to Plaintiffs and Class Members.

24 217. As a direct and proximate result of Defendant's trespass to chattels,  
25 nuisance, interference, unauthorized access of and intermeddling with Plaintiffs'  
26 and Class Members' property, Defendant has injured and impaired in the condition  
27 and value of Class Members' computers, as follows:

28 a) By consuming the resources of and/or degrading the performance

- 1 of Plaintiffs' and Class Members' computers (including hard drive  
2 space, memory, processing cycles, and Internet connectivity);
- 3 b) By diminishing the use of, value, speed, capacity, and/or  
4 capabilities of Plaintiffs' and Class Members' computers;
- 5 c) By devaluing, interfering with, and/or diminishing Plaintiffs' and  
6 Class Members' possessory interest in their computers;
- 7 d) By altering and controlling the functioning of Plaintiffs' and Class  
8 Members' computers;
- 9 e) By infringing on Plaintiffs' and Class Members' right to exclude  
10 others from their computers;
- 11 f) By infringing on Plaintiffs' and Class Members' right to  
12 determine, as owners of their computers, which programs should  
13 be installed and operating on their computers;
- 14 g) By compromising the integrity, security, and ownership of Class  
15 Members' computers; and
- 16 h) By forcing Plaintiffs and Class Members' to expend money, time,  
17 and resources in order to remove the program installed on their  
18 computers without notice or consent.

19 **Count VII**  
20 **Unjust Enrichment**  
21 **By All Plaintiffs against Defendant**

22 218. Plaintiffs incorporate the above allegations by reference as if set forth  
23 herein at length.

24 219. Plaintiffs assert this claim against Defendant named herein in this  
25 complaint on behalf of themselves and the Class.

26 220. A benefit has been conferred upon all Defendants by Plaintiffs and the  
27 Class. On information and belief, Defendant, directly or indirectly, have received  
28 and retain information regarding online communications and activity of Plaintiffs,



1 and Defendant has received and retain information regarding specific purchase and  
2 transactional information that is otherwise private, confidential, and not of public  
3 record, and/or have received revenue from the provision of such information.

4 221. Defendant appreciate or have knowledge of said benefit.

5 222. Under principles of equity and good conscience, Defendants should  
6 not be permitted to retain the information and/or revenue which they acquired by  
7 virtue of their unlawful conduct. All funds, revenues, and benefits received by  
8 Defendant rightfully belong to Plaintiffs and the Class, which Defendants have  
9 unjustly received as a result of its actions.

#### 10 **PRAYER FOR RELIEF**

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

- 13 A. Certify this case as a Class action on behalf of the Classes defined above,  
14 appoint Plaintiffs as Class representatives, and appoint their counsel as Class  
15 counsel;
- 16 B. Declare that the actions of Defendant, as set out above, violate the  
17 following:
- 18 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
  - 19 b) California's Computer Crime Law, Penal Code § 502;
  - 20 c) California's Invasion Of Privacy Act, California Penal Code § 630;
  - 21 d) California's Consumer Legal Remedies Act, Civil Code § 1750;
  - 22 e) California's Unfair Competition Law, Business and Professions Code  
23 § 17200;
  - 24 f) Trespass to Personal Property / Chattels;
  - 25 g) Unjust Enrichment
- 26  
27  
28

1 C. As applicable to the Classes *mutatis mutandis*, awarding injunctive and  
2 equitable relief including, *inter alia*: (i) prohibiting Defendant from  
3 engaging in the acts alleged above; (ii) requiring Defendant to disgorge all  
4 of its ill-gotten gains to Plaintiffs and the other Class Members, or to  
5 whomever the Court deems appropriate; (iii) requiring Defendant to delete  
6 all data surreptitiously or otherwise collected through the acts alleged above;  
7 (iv) requiring Defendant to provide Plaintiffs and the other Class Members a  
8 means to easily and permanently decline any participation in any data  
9 collection activities; (v) awarding Plaintiffs and Class Members full  
10 restitution of all benefits wrongfully acquired by Defendant by means of the  
11 wrongful conduct alleged herein; and (vi) ordering an accounting and  
12 constructive trust imposed on the data, funds, or other assets obtained by  
13 unlawful means as alleged above, to avoid dissipation, fraudulent transfers,  
14 and/or concealment of such assets by Defendant;

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

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

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

23 G. Award Plaintiffs and the Classes:

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

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

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

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

e) statutory damages, including punitive damages;

1 f) permanent injunction prohibiting Defendant from engaging in the  
2 conduct and practices complained of herein;  
3

4 H. For such other and further relief as this Court may deem just and proper.  
5

6 Dated this 17<sup>th</sup> day of August 2010  
7

8   
By: David Parisi

9 David Parisi (SBN 162248)

10 [dcparsi@parisihavens.com](mailto:dcparsi@parisihavens.com)

11 Parisi & Havens LLP

12 15233 Valleyheart Drive

13 Sherman Oaks, California 91403

Telephone: (818) 990-1299

14 Joseph H. Malley (not admitted)

15 malleylaw@gmail.com

16 Law Office of Joseph H. Malley

17 1045 North Zang Blvd

Dallas, TX 75208

18 Telephone: (214) 943-6100  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**JURY TRIAL DEMAND**

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

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

Dated this 17<sup>th</sup> day of August 2010

  
By: David Parisi

David Parisi (SBN 162248)  
dcparisi@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





**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET**

**VIII(a). IDENTICAL CASES:** Has this action been previously filed in this court and dismissed, remanded or closed?  No  Yes  
If yes, list case number(s): \_\_\_\_\_

**VIII(b). RELATED CASES:** Have any cases been previously filed in this court that are related to the present case?  No  Yes  
If yes, list case number(s): 2:10-cv-05484-GW

**Civil cases are deemed related if a previously filed case and the present case:**

- (Check all boxes that apply)  A. Arise from the same or closely related transactions, happenings, or events; or  
 B. Call for determination of the same or substantially related or similar questions of law and fact; or  
 C. For other reasons would entail substantial duplication of labor if heard by different judges; or  
 D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

**IX. VENUE:** (When completing the following information, use an additional sheet if necessary.)

(a) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which EACH named plaintiff resides.  
 Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles	Other States: Texas; Nevada

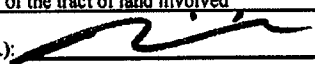
(b) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which EACH named defendant resides.  
 Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Orange County	

(c) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which EACH claim arose.  
**Note: In land condemnation cases, use the location of the tract of land involved.**

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles	Other States: Texas; Nevada

\* Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties  
**Note: In land condemnation cases, use the location of the tract of land involved**

X. SIGNATURE OF ATTORNEY (OR PRO PER):  Date August 17, 2010

**Notice to Counsel/Parties:** The CV-71 (JS-44) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

**Key to Statistical codes relating to Social Security Cases:**

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

**NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY**

This case has been assigned to District Judge James V. Selna and the assigned discovery Magistrate Judge is Victor B. Kenton.

The case number on all documents filed with the Court should read as follows:

**SACV10- 1256 JVS (VBKx)**

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

=====

**NOTICE TO COUNSEL**

*A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).*

Subsequent documents must be filed at the following location:

**Western Division**  
312 N. Spring St., Rm. G-8  
Los Angeles, CA 90012

**Southern Division**  
411 West Fourth St., Rm. 1-053  
Santa Ana, CA 92701-4516

**Eastern Division**  
3470 Twelfth St., Rm. 134  
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.



Name & Address:  
David C. Parisi (SBN 162248)  
Parisi & Havens LLP  
15233 Valleyheart Drive  
Sherman Oaks, California 91403  
Telephone: (818) 990-1299

FOR OFFICE USE ONLY

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

GENEVIVE LA COURT; See attachment A for  
additional plaintiffs

CASE NUMBER

PLAINTIFF(S)

SACV10-01256 JVS VBKx

v.

SPECIFIC MEDIA, INC., a Delaware Corporation,

SUMMONS

DEFENDANT(S).

TO: DEFENDANT(S): \_\_\_\_\_

A lawsuit has been filed against you.

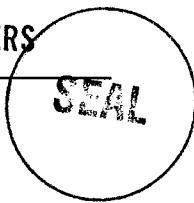
Within 21 days after service of this summons on you (not counting the day you received it), you must serve on the plaintiff an answer to the attached  complaint  \_\_\_\_\_ amended complaint  counterclaim  cross-claim or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff's attorney, David C. Parisi, whose address is Parisi & Havens LLP, 15233 Valleyheart Drive, Sherman Oaks, California 91403. If you fail to do so, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Clerk, U.S. District Court

Dated: AUG 19 2010

By: CHRISTOPHER POWERS  
Deputy Clerk

(Seal of the Court)



FOR OFFICE USE ONLY

[Use 60 days if the defendant is the United States or a United States agency, or is an officer or employee of the United States. Allowed 60 days by Rule 12(a)(3)].

**ATTCHMENT A**

Attachment to Summons

Case Number: \_\_\_\_\_

**Additional Plaintiffs:**

DEIRDRE HARRIS; CAHILL HOOKER; BILL LATHROP; JUDY  
STOUGH; and E.H., a minor, by and through her parent, JEFF HALL;  
individuals, on behalf of themselves and others similarly situated

**ATTACHMENT A**

**Attachment to Summons**